EP・US　　特許協力条約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号 S00P1369W000	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０７６８２	国際出願日 （日.月.年）　０１．１１．００	優先日 （日.月.年）　０１．１１．９９
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☒ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　6　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]　　国際出願番[redacted]PCT／JP00／07682

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－１１は、共通アドレスの利用による同報の制御に関するものである。

請求の範囲１２－２５は、宛先テーブルのエントリの有効情報による送信制御に関するものである。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年5月10日 (10.05.2001)

PCT

(10) 国際公開番号
WO 01/33771 A1

(51) 国際特許分類[7]: H04L 12/18, 9/36, 9/32, H04H 1/00, H04N 7/16

(21) 国際出願番号: PCT/JP00/07682

(22) 国際出願日: 2000年11月1日 (01.11.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/311651 1999年11月1日 (01.11.1999) JP
特願平11/314521 1999年11月5日 (05.11.1999) JP

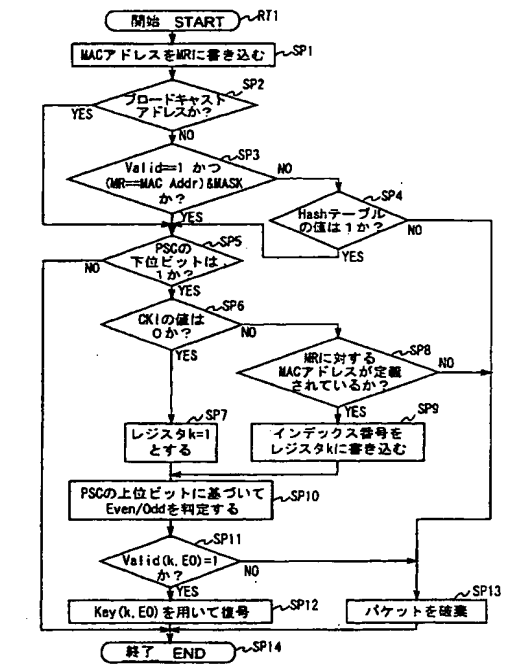
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 赤地正光 (AKACHI, Masateru) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

[続葉有]

(54) Title: INFORMATION TRANSMISSION SYSTEM AND METHOD, TRANSMITTER AND RECEIVER, DATA PROCESSING DEVICE AND DATA PROCESSING METHOD, AND RECORDED MEDIUM

(54) 発明の名称: 情報伝送システム及び方法、送信装置及び受信装置、データ処理装置およびデータ処理方法、並びに記録媒体



SP1...WRITE MAC ADDRESS INTO MR
SP2...BROADCAST ADDRESS ?
SP3...VALID==1 AND (MR==MAC Addr) & MASK ?
SP4...IS VALUE OF HASH TABLE 1 ?
SP5...IS LOW-ORDER BIT OF PSC 1 ?
SP6...IS VALUE OF CKI 0 ?
SP7...SET REGISTER K AT 1
SP8...IS MAC ADDRESS FOR MR DEFINED ?
SP9...WRITE INDEX NUMBER INTO REGISTER K
SP10...JUDGE Even/Odd ACCORDING TO UPPER-ORDER BIT OF PSC
SP11...Valid (k, EO) = 1 ?
SP12...DECODE USING Key (k, EO)
SP13...DISCARD PACKET

(57) Abstract: When data is transmitted to a receiver piece by piece, the address specifically allocated to the receiver is added to the data and transmitted together. When common data is transmitted to an arbitrary group of receivers, a set of common address information representing the common part of addresses of the receivers and a set of address range information specifying the range of the common part of the addresses are added to the data and transmitted together. When the transmitted data is received, the specific address is compared with the address added to the data. If the specific address agrees with the address added to the data, or if the specific address partially agrees with the common address information to which the data is added in the range indicated by the address range information, the data is decoded.

WO 01/33771 A1

[続葉有]

(74) 代理人: 弁理士　田辺恵基(TANABE, Shigemoto); 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンフアンタジアビル5階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、当該データを復号するようにした。

明　細　書

情報伝送システム及び方法、送信装置及び受信装置、データ処理装置およびデータ処理方法、並びに記録媒体

技術分野

本発明は情報伝送システム及び方法、送信装置及び受信装置に関し、例えば衛星を介して情報を伝送する情報伝送システムに適用して好適なものである。また、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、例えば、データを、衛星回線等によって同報する場合に、そのデータを取得することのできる端末（ユーザ）を、容易に制限することができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

背景技術

従来ディジタル衛星放送システムにおいては、受信契約を行った正当な受信者のみが放送を受信し得る限定受信機構（ＣＡ：ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ）が用いられている。

かかる限定受信機構においては、受信契約を行った受信者に対して予め所定の秘密鍵を渡しておく。送信側はこの秘密鍵を用いて放送データを暗号化し、放送衛星を介して送信する。そして受信者は秘密鍵を用いて受信波の暗号化を解除することにより、受信契約を行った受信者のみが放送を視聴し得るようになされている。

ここで近年、ディジタル衛星放送システムを用いてデータ伝送を行う、衛星データ伝送システムが考えられている。衛星回線は電話回線やＩＳＤＮ回線等に比べてその通信速度が速いため、大容量データを短時間で伝送することができという利点がある。

この衛星データ伝送システムにおいて、各受信者に対して個別のデータを伝送

する個別通信（以下、これをユニキャストと呼ぶ）ことに加えて、全ての受信者に対して同一のデータを伝送する同報通信（以下、これをブロードキャストと呼ぶ）や、任意の受信者グループに対して同一のデータを伝送するグループ通信（以下、これをマルチキャストと呼ぶ）等の様々な受信制御を行うことができれば、衛星データ伝送システムの使い勝手がより一層向上すると考えられる。

ところがかかる限定受信機構においては、全受信者が常に同じ情報を受信して視聴することを前提として設計されているため、ユニキャストやマルチキャスト等の受信制御を行い得ないという問題があった。

また、例えば、画像や音声等をディジタルデータで伝送する場合には、アナログ信号で伝送する場合と同一の伝送帯域で複数チャンネルを確保したり、また、より高品質の画像や音声を提供することが可能であり、衛星放送あるいは衛星通信等の分野では、画像や音声をディジタルデータで提供するシステムの普及が進んでいる。例えば、国内ではＳｋｙＰｅｒｆｅｃＴＶ！やＤｉｒｅｃＴＶ、北米ではＤｉｒｅｃＴＶ、欧州ではＣａｎａｌ　Ｐｌｕｓ、といったディジタル衛星放送サービスが、それぞれ開始されている。放送のディジタル化は、１チャンネル当たりの送信コストの低減や、コンピュータで扱われるプログラムやデータの提供等を可能とし、また、ディジタル化により、プログラム等と画像等とを連動して提供するようなサービスも普及しつつある。

ディジタル衛星放送サービスでは、画像や音声のディジタルデータが、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ)2や、このＭＰＥＧ２から派生したＤＶＢ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ）の規格に準拠したフォーマットに変換され、さらに多重化されて、電波として送信される。電波は、衛星のトランスポンダで受信され、増幅その他の必要な処理が施された後、地上に向けて送出される。

トランスポンダの伝送帯域は、例えば、３０Ｍｂｐｓ（Ｍｅｇａ　ｂｉｔ　ｐｅｒ　ｓｅｃｏｎｄ）と大きく（但し、トランスポンダでは、一般に、エラー訂正符号が付加されるので、３０Ｍｂｐｓの伝送帯域を有していても、実質的な

伝送帯域は、最大で２７Ｍｂｐｓ程度)、このような大きな伝送帯域の全部を利用することで、ディジタルデータを、高品位で、かつ高速に配信することが可能である。

しかしながら、一般には、主に、コスト上の理由から、トランスポンダの伝送帯域は、多チャンネルに分割されて使用されることが多い。この場合、各チャンネルで伝送されるディジタルデータの内容は異なっていても、各チャンネルのディジタルデータを受信する受信側の仕組みは共通であるため、あるディジタルデータの提供を、特定のユーザだけが受けることができるような限定受信（ＣＡ（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ））機構が必要となる。

即ち、特に、例えば、いわゆるデータ放送を行う場合には、画像や音声を配信する場合に比較して、１番組当たりのデータ量が小さく、課金単位あるいは課金形態が複雑になることが予想され、これに対処するには、より細かな受信制御を行うことができる限定受信機構が必要となる。また、限定受信機構は、機密情報を配信する場合にも、その漏洩を防止するために必要となる。

一般に、限定受信機構は、配信するデータストリームに対して暗号化を施すことによって実現される。暗号化方式としては、大きく分けて、共通鍵暗号化方式（秘密鍵暗号化方式）と、公開鍵暗号化方式とが知られている。ディジタル衛星放送では、暗号化／復号の処理の負荷が、公開鍵暗号化方式に比較して軽いことから、共通鍵暗号化方式が用いられることが多い。

共通鍵暗号化方式では、ある契約者Ａに対して、暗号鍵と同一の、復号鍵となる符号列を何らかの方法で渡し、データが、暗号鍵で暗号化されて配信される。暗号化されたデータは、それから、暗号鍵（復号鍵）や元のデータを逆計算する等して類推することが困難なようになっており、従って、契約者でないユーザＢは、暗号化されたデータを受信しても、それを、元のデータに正しく復元することはできない。また、契約者であるユーザＡは、暗号化されたデータを、契約することにより渡された復号鍵で復号することにより、元のデータを復元することができる。従って、受信契約とは、復号鍵の引き渡しを行うことと等価である。

ところで、例えば、いま、ユーザＡとＣが契約者である場合において、ユーザＡだけとの契約が終了したり、あるいは、ユーザＡが不正な行為をしたときには、いままで使用していた暗号鍵を変更し、その変更後の暗号鍵と同一の復号鍵を、ユーザＣのみに提供すれば、その後は、契約者でなくなった、あるいは不正な行為を行ったユーザＡは、新たな暗号鍵で暗号化されたデータを復元することができなくなるとともに、正当な契約者であるユーザＣは、続けて、新たな暗号鍵で暗号化されたデータを、新たな復号鍵で復号することにより正常に復元することができる。

しかしながら、あるユーザの契約が終了したり、不正な行為を発見するごとに、暗号鍵を変更し、さらに、変更後の暗号鍵と同一の復号鍵を、正当な契約者に提供するのは面倒である。

発明の開示

本発明は以上の点を考慮してなされたもので、様々な受信制御を行い得る情報伝送システム及び方法、送信装置及び受信装置を提案しようとするものである。

また、データを正常に取得する（受信する）ことのできるユーザを、容易に制限することができるようにするものである。

かかる課題を解決するため本発明においては、送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信するとともに、送信されたデータを受信し、固有のアドレスと当該データに付せられたアドレスとが一致したとき、又は固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較して比較結果が一致したとき、

当該データを復号するようにした。

任意のグループの受信装置に対して共通のデータを送信するとき、当該任意のグループの受信装置間で共通するアドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信し、受信装置では固有のアドレスと当該データに付せられた共通アドレス情報とをアドレス範囲情報が示す範囲で比較し、比較結果が一致したとき当該データを復号するようにしたことにより、簡易な構成で様々な受信制御を行い得る。

本発明のデータ処理装置は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定手段と、判定手段による判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御手段とを備えることを特徴とする。

出力制御手段には、注目エントリが有効である場合に、データを、データブロックに配置された宛先に出力させ、注目エントリが有効でない場合に、データを破棄させることができる。

データが暗号化されている場合には、データ処理装置には、暗号化されたデータを復号する復号手段をさらに設けることができる。

データが、そのデータの宛先に割り当てられた鍵を用いて暗号化され、テーブルの各エントリに、宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されている場合には、復号手段には、テーブルに登録されている鍵を用いて、データを復号させることができる。

復号手段には、テーブルの、データブロックの宛先に割り当てられた鍵を用いて、そのデータブロックに配置されたデータを復号させることができる。

テーブルの各エントリに、宛先、エントリ有効情報、および鍵の他、その鍵が

有効かどうかを表す鍵有効情報も登録されている場合には、復号手段には、データブロックの宛先に割り当てられた鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定させ、有効であるときに、鍵を用いて、データを復号させることができる。

テーブルの各エントリには、宛先およびエントリ有効情報の他、その宛先に割り当てられた２以上の鍵も登録することができる。

テーブルの各エントリには、２以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報も登録することができる。

本発明のデータ処理装置には、テーブルを記憶するテーブル記憶手段をさらに設けることができる。

宛先は、データを受信すべき通信端末のＭＡＣ(（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスとすることができる。

データブロックは、ＤＶＢ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ）の規格に準拠したものとすることができる。

本発明のデータ処理装置は、１チップのＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）で構成することができる。

本発明のデータ処理方法は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えることを特徴とする。

本発明の記録媒体は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有する

エントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えるプログラムが記録されていることを特徴とする。

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかが判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかが判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。従って、データを正常に取得することのできるユーザを、容易に制限することが可能となる。

図面の簡単な説明

図１は、本発明による衛星データ伝送システムの全体構成を示すブロック図である。

図２は、受信装置の回路構成を示すブロック図である。

図３は、ヘッダフォーマットを示す略線図である。

図４は、マスクとＭＡＣアドレスの関係を示す略線図である。

図５は、鍵テーブルのデータ構成を示す略線図である。

図６は、復号処理を示すフローチャートである。

図７は、本発明を適用した放送システムの一実施の形態の構成例を示すブロック図である。

図８は、図７の送信システム１０１の処理を説明するためのフローチャートである。

図９は、セクションとセクションヘッダのフォーマットを示す図である。

図１０は、図７の受信装置１２２の構成例を示すブロック図である。

図１１は、鍵テーブルを示す図である。

図１２は、図１０の受信装置１２２の処理を説明するためのフローチャートである。

図１３は、本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

発明を実施するための最良の形態

以下図面について本発明の一実施の形態を詳述する。

（１）第１の実施の形態

（１－１）衛星データ伝送システムの全体構成

図１において、１は全体として本発明を適用した衛星データ伝送システムを示し、送信側システム２、衛星３、及び複数の同一構成でなる受信側システム４で構成される。送信側システム２と各受信側システム４とはそれぞれインターネット５を介して接続されている。また送信側システム２を管理するサービスプロバイダと各受信側システム４を所有する受信者との間では、予め当該衛星データ伝送システム１についての利用契約が結ばれている。

送信側システム２においては、当該送信側システム２全体を制御する制御装置１０、回線接続装置１１、データサーバ１２及び送信処理装置１３がローカルネットワーク１４を介して接続されている。

制御装置１０は、受信側装置４が有する情報処理装置２２から送信されたデータ読出要求を、回線接続装置１１を介して受信する。そして制御装置１０はデータ読出要求に応じて、データサーバ１２或いはインターネット５上のデータサーバ（図示せず）からデータを読み出し、送信処理装置１３に供給する。

ここで送信処理装置１３は、受信側装置４の各情報処理装置２２に付せられた固有の識別番号であるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ：メディアアクセス制御）アドレスと、当該ＭＡＣアドレスに対応して設定された秘密鍵とを記述した暗号鍵対応表を有している。そして送信処理装置１３は秘密鍵対応表に基づいて、読み出されたデータをデータ送信先の情報処理装置２２のＭＡＣアドレスに対応した秘密鍵を用いてデータを暗号化する。また送信処理装置１３は、ブロードキャストとして全ての情報処理装置２２に送信するデータについて、当該データのＣＫＩ（Ｃｏｍｍｏｎ　Ｋｅｙ　Ｉｎｄｉｃａｔｏｒ、後述）の値を”０”とするとともに、所定の共通鍵を用いて暗号化する。そして送信処理装置１３は、暗号化したデータをＤＶＢ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ）データ放送仕様に定める形式でパケット化し、アップリンク波Ｓ２として送信１５を介して衛星３に送信する。

衛星３はアップリンク波Ｓ２を受信して増幅し、ダウンリンク波Ｓ３として地上の受信側システム４に向けて再送信する。

受信側システム４においては、受信装置２１、回線接続装置２３、及び、例えばパーソナルコンピュータ等でなる複数の情報処理装置２２が、ローカルネットワーク２４を介して相互に接続されている。

受信装置２１は、受信アンテナ２０を介して受信したダウンリンク波Ｓ３に対して復調処理及び後述する復号処理を行うことにより、情報処理装置２２に向けに送信されたデータを復号し、ローカルネットワーク２４を介して、当該情報処理装置２２に供給する。

また情報処理装置２２は、ユーザによってデータの読出要求操作が入力されると、これに応じてデータの読出要求を回線接続装置２３及びインターネット５を

介して送信側システム２に送信する。

（１－２）受信装置の構成

次に、受信側システム４の受信装置２１を図２を用いて説明する。

受信装置２１においては、当該受信装置２１全体を制御するＣＰＵ（Ｃｅｎ－ｔｒａｌ　Ｐｒｏｓｓｅｃｉｎｇ　Ｕｎｉｔ）３０に、バス３９を介してフロントエンド部３１、分離部３２、受信フィルタ３３、復号部３４、チェッカ３５、バッファ３６、鍵テーブル３７及びインターフェース部３８が接続されている。

フロントエンド部３１は、受信アンテナ３９を介して受信したダウンリンク波Ｓ３を復調し、データストリームＤ３１としてデマルチプレクサ３２に供給する。デマルチプレクサ３２は、ＰＩＤ（Ｐａｃｋｅｔ　ＩＤ）に基づいて、データストリームＤ３１から必要なパケットのみを分離して受信フィルタ３３に供給する。受信フィルタ３３は、デマルチプレクサ３２から供給されたパケットのペイロード内容を調べ、データ復号処理に不要なパケットを破棄する。

復号部３４は後述する復号処理に基づいて動作し、情報処理装置２２（図１）のＭＡＣアドレスを検索キーにして鍵テーブル２８に問い合わせを行い、当該鍵テーブル２８から復号鍵を取得する。そして復号部３４は、取得した復号鍵を用いてデータストリームＤ３１を復号し、復号データＤ３４としてチェッカ３５に供給する。

チェッカ３５は、復号データＤ３４に対して復号処理が正常に行われたか否かの検査を行い、正常に復号されたパケットのみをバッファ３６に供給する。そしてバッファ３６はＣＰＵ３０の要求に応じて、復号データＤ３４をバス３９を介してインターフェイス部３８に読み出す。インターフェイス部３８は、復号データＤ３４をローカルネットワーク２４（図１）を介して情報処理装置２２に供給する。

かくして受信装置２１はダウンリンク波Ｓ３を受信し、情報処理装置２２向けに供給されたデータのみを取り出して当該情報処理装置２２に供給する。

（１－３）ディジタルストリームの復号処理

ディジタルストリームＤ３１は、図３に示すように、ペイロードの先頭にパケットヘッダ情報が付加されるとともに、ペイロードの末尾にスタッフィングバイト（無効バイト）及びＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｏｄｅ：巡回冗長符号）が付加され、ＤＶＢデータ放送仕様に定めるセッションとして処理可能な形態（Ｄａｔａｇｒａｍ－ｓｅｃｔｉｏｎ）にカプセル化されて構成される。ここでＭＡＣアドレス＃６とは、ＭＡＣアドレスの最上位ビットをＢｉｔ４７、最下位ビットをＢｉｔ０としたときの、Ｂｉｔ７からＢｉｔ０を含むバイト（８ｂｉｔ）を意味する。

復号部３４においては、まず受信したデータストリームＤ３１の各パケットに記述されたＭＡＣアドレスと鍵テーブル３７とに基づいて、当該パケットを受信するべきか否かを弁別する。

ここで本発明による受信装置２１は、かかるパケット弁別処理において、ＭＡＣアドレスにおける比較すべきビット位置を指定するマスクビット処理と、ＭＡＣアドレスをより少ないビット数の数値に変換し、これを用いてパケットの弁別を行うＭＡＣアドレス変換処理と、特定のＭＡＣアドレスを有するパケットを無条件で通過させるＭＡＣアドレス通過処理とを実行する。

マスクビット処理は、セクションヘッダに記述されたＭＡＣアドレスと鍵テーブル３７のＭＡＣアドレスの比較演算による状態判定に、マスクビットと比較演算結果の論理積演算を付加するものであり、排他論理和を＾、論理積を＆で表し、セッションヘッダ記載のＭＡＣアドレスをＭＲ、鍵テーブルｋ番めのＭＡＣアドレスをＭＡＣ（ｋ）、ビットの重みを１と表すとすると、各ビット毎に

$$(\sim (MR_1 \hat{} MAC_1 (k)) \& MASK_1 (k) \quad \cdots\cdots (1)$$

なる演算を０≦ｌ≦４７なる範囲で全てのビットに対して行い、この結果が全て

”０”である場合にＭＡＣアドレスが合致したとするものである。

これはすなわち、マスクが”１”であるビットにおいてのみＭＲとＭＡＣアドレスの比較を行うということである。このマスクビットとＭＲ及びＭＡＣアドレスの比較操作との関係を図４に示す。

図４の場合、マスクビットはＤ０～Ｄ３までが”０”であり、Ｄ４～Ｄ４７は”１”である。かかるマスクビットを用いてＭＡＣアドレスの照合を行う場合、マスクビットが”１”であるＤ４～Ｄ４７の区間において、ＭＡＣアドレスとＭＲが同一であることがＭＡＣアドレスの合致条件であり、マスクビットが”０”であるＤ０～Ｄ３の区間は、ＭＡＣアドレスとＭＲが同一でなくてもかまわない。このようにマスクビットを用いてＭＡＣアドレスの一部のみを照合することにより、それぞれ異なるＭＡＣアドレスを有する任意の情報処理装置２２に対して同一のパケットを配信するマルチキャスト（グループ通信）を行うことができる。またマスクビットを全て”１”、即ち”０ｘＦＦＦＦＦＦＦＦＦＦＦＦ”とすることにより、ＭＡＣアドレス全てのビットに対して照合が行われ、ユニキャスト（個別通信）を行うことができる。

ここで、マスクビットを用いてマルチキャストを行う場合、各情報処理装置２２のＭＡＣアドレスに共通部分が存在することが前提となるが、そのように情報処理装置２２を揃えることは難しく、またシステムを運用する際の柔軟さを欠くことにもなる。この場合、実際の情報処理装置２２のＭＡＣアドレスとパケットヘッダに記述されるＭＡＣアドレスとの対応表に基づいて、パケットヘッダを書き換えて疑似的にＭＡＣアドレスの共通部分を作り出すようにすればよい。

ＭＡＣアドレス変換処理は、入力したＭＡＣアドレスに対してある種の計算式（ハッシュ関数）による演算を行い、４８ビット以下のビット数に縮小した数値を得、これをキーにして通過させるか否かを記述したテーブル（ハッシュテーブル）を参照するものである。このビット数の縮小は、ハッシュテーブルを小さくするためである。ハッシュ関数は入力されるＭＡＣアドレスをよく分散させるような関数であれば何でも良く、例えばＭＡＣアドレスのＣＲＣを求め、この上位

６ビットをｐとし、Ｐａｓｓ（ｐ）が”１”であれば通過させ、例えば”０”であれば破棄する。ここでｐａｓｓは2^6＝６４ビットのテーブルである。このようにハッシュ関数を用いてＭＡＣアドレスのビット数を縮小することにより、復号部３４の回路規模を小さくすることができる。

またＭＡＣアドレス通過処理は、パケットのヘッダに記述されたＭＡＣアドレスが所定の同報通信用のアドレスである場合、鍵テーブルの状態に関わらず通過させるというものであり、例えばパケットのヘッダ記載のＭＡＣアドレスが”０ｘＦＦＦＦＦＦＦＦＦＦＦＦ”（このアドレスをブロードキャストアドレスと呼ぶ）であれば常に同報通信（ブロードキャスト）とみなしてこれを通過させる。本発明においては、かかるＭＡＣアドレス通過処理をマスクビット処理及びＭＡＣアドレス変換処理に先行して実行する。これによりパケットヘッダ記載のＭＡＣアドレスがブロードキャストアドレスである場合鍵テーブルの検索が不要になり、処理速度が向上するという効果がある。

かくして復号部３４は、パケットのヘッダに記述されたＭＡＣアドレス、情報処理装置２１のＭＡＣアドレス、及びマスクビットに基づいてパケットの弁別を行う。

続いて復号部３４は、弁別されたパケットが暗号化されているかを検出する。そしてパケットが暗号化されているときは、復号鍵を鍵テーブルより取り出して復号処理を行うが、同報通信においては複数のＭＡＣアドレスで共用する復号鍵である共通鍵を具備する必要がある。

本発明による受信装置２１では、共通鍵を使用するか否かを、例えばセクション６バイト目の最上位ビット（図３の２行めの第２番目のバイトのＤ７）を用いて判断する。これを本発明ではＣＫＩ（Ｃｏｍｍｏｎ　Ｋｅｙ　Ｉｎｄｉｃａｔｏｒ）と呼ぶ。そしてＣＫＩが”１”であれば、ＭＲ、ＭＡＣアドレス及びマスクビットによって鍵テーブルから抽出される個別鍵を使用し、ＣＫＩが”０”であれば、鍵テーブルの設定にかかわらず共通鍵を使用すると定める。ここで、ＤＶＢデータ放送仕様においてはＣＫＩはｒｅｓｅｒｖｅｄとされており、値と

して”１”をとることになっている。共通鍵は個別鍵に比べてより特殊な処理方法であると考えられるので、ＣＫＩが”０”である場合に共通鍵を使用すると定めることで、ＤＶＢデータ放送仕様との仕様を一致することができる。

共通鍵は特定の記憶領域を用意しても良いが、鍵テーブル中の特定の行のデータを兼用すれば処理が個別鍵と共通化でき、記憶領域も有効に利用できるのでより望ましい。この特定の行としてより好ましくは先頭の行、即ち第１行を指定する。鍵テーブルの行数ｎがいくつであれ必ず第１行めは存在するので、このようにすればｎの値が異なる受信装置であっても処理手順を変えることなく共通鍵の記憶又は取り出しを行うことができる。

図５は鍵テーブルの構成を示し、ＭＡＣアドレス＃１は鍵テーブルの第１番行に記述されたＭＡＣアドレスを、マスク＃１はＭＡＣアドレス＃１に対応するマスクビットを、K_{1Even} 、K_{1Odd}は各々ＭＡＣアドレス＃１に対応づけれたＥｖｅｎ／Ｏｄｄの鍵データを意味しており、使用する暗号形式に応じたビット幅ｍを持つ。鍵テーブルは上記と同様の構造を複数（ｎ個）持っている。この最大数は鍵テーブル２８が持ちうる回路規模から上限が決定される。

ＭＡＣアドレスと鍵データはそれぞれ独立したＶａｌｉｄフラグを有しており、これにより個別に値が有効であるか無効であるかを管理することができるようになされており、当該Ｖａｌｉｄフラグを、ＭＡＣアドレス弁別に流用することも可能になる。また、鍵テーブルは各行毎に独立したＶａｌｉｄフラグを有しているため、当該鍵テーブルは空行（無効な行）を含んでいても良く、これにより一時的に特定の行の情報を無効にしたい場合、単にＭＡＣアドレスのＶａｌｉｄビットを”０”にするだけでよく、高速な処理のために好適である。

復号部３４は、かくして得られた復号鍵を用いてパケットの復号を行う。

（１－４）復号処理手順

次に、ディジタルストリームの復号処理手順を図６の流れ図に示しながら説明する。

復号部３４はＲＴ１で処理を開始し、ステップＳＰ１において、パケットヘッダに記述されている４８ｂｉｔのＭＡＣアドレスをレジスタＭＲに読み込み、次のステップＳＰ２に進む。

ステップＳＰ２において、復号部３４はレジスタＭＲの値がブロードキャストアドレス（０ｘＦＦＦＦＦＦＦＦＦＦＦＦ）に等しいか否かを判断する。ステップＳＰ２において肯定結果が得られた場合、このことはレジスタＭＲの値がブロードキャストアドレスに等しいこと、すなわち当該パケットがブロードキャストパケットであることを表しており、復号部３４はステップＳＰ３及びＳＰ４をスキップし、ステップＳＰ５に進む。

これに対してステップＳＰ２において否定結果が得られた場合、このことはレジスタＭＲの値がブロードキャストアドレスに等しくないこと、すなわち当該パケットがブロードキャストパケットではないことを表しており、復号部３４はステップＳＰ３に進む。

ステップＳＰ３において、復号部３４は鍵テーブル３７内に、Ｖａｌｉｄビットが”１”（すなわち有効状態）であるとともに、マスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在するか否かを、（１）式に基づいて鍵テーブルを＃１行から順に各行検索する。

ステップＳＰ３において肯定結果が得られた場合、このことは有効状態かつマスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在したことを表しており、復号部３４はステップＳＰ５に進む。

これに対してステップＳＰ３において否定結果が得られた場合、このことは有効状態かつマスクビットが”１”である区間の全ビットにおいてレジスタＭＲとＭＡＣアドレスとが等しい行が存在しないことを表しており、復号部３４はステ４に進む。

ステップＳＰ４において、復号部３４は、ハッシュ関数を用いてパケットヘッダに記載のＭＡＣアドレスからハッシュ値を生成し、当該ハッシュ値を用いて所

定のハッシュテーブルを検索し、ハッシュ値に対応するビットが”１”であるか否かを判断する。

ステップＳＰ４において否定結果が得られた場合、このことはハッシュテーブルのビットが”０”であり、当該パケットは受信装置２１が受信すべきパケットではないことを表しており、復号部３４はステップＳＰ１３に進み、当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

これに対してステップＳＰ４において肯定結果が得られた場合、このことはハッシュテーブルのビットが”１”であり、当該パケットは受信装置２１が受信すべきパケットであることを表しており、復号部３４はステップＳＰ５に進む。

ステップＳＰ５において、復号部３４は、パケットヘッダにおけるＰＳＣ（Ｐａｙｌｏａｄ　Ｓｃｒａｍｂｌｉｎｇ　Ｃｏｎｔｒｏｌ）（図３）の下位ビットの値に基づいて、当該パケットが暗号化されているか否かを判断する。ステップＳＰ５において否定結果が得られた場合、このことは下位ビットが”０”であること、すなわち当該パケットが暗号化されていないことを表しており、復号部３４はステップＳＰ１４へ進み、暗号解除処理を行わずにパケットを後段のチェッカ３５に送出し処理を終了する。

これに対してステップＳＰ５において肯定結果が得られた場合、このことは下位ビットが”１”であること、すなわち当該パケットが暗号化されていることを表しており、復号部３４はステップＳＰ６に進む。

ステップＳＰ６において、復号部３４は、パケットヘッダにおけるＣＫＩ（図３）の値に基づいて、当該パケットが共通鍵を用いて暗号化されているか否かを判断する。ステップＳＰ６において肯定結果が得られた場合、このことはＣＫＩが”０”であること、すなわち当該パケットが共通鍵を用いて暗号化されていることを表しており、復号部３４はステップＳＰ７へ進み、鍵の索引番号を記憶するレジスタｋに共通鍵を示す”１”を代入し、ステップＳＰ１０に進む。

これに対してステップＳＰ６において否定結果が得られた場合、このことはＣＫＩが”１”であること、すなわち当該パケットが個別鍵を用いて暗号化されて

いることを表しており、復号部３４はステップＳＰ８に進む。

ステップＳＰ８において、復号部３４は鍵テーブルを（１）式に基づいて各行順次検索し、ＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在するか否かを判断する。ここで、ステップＳＰ４におけるハッシュテーブルによる弁別では受信すべきではないパケットもたまたまハッシュ値が合致すれば通過させてしまうが、このようなパケットは当該ステップＳＰ８にて再度弁別されるため、誤って復号処理されることはない。ちなみに、暗号化されていないパケットはステップＳＰ８を通過しないので、これは後段回路あるいは情報処理装置２２にて破棄する。

鍵テーブルの探索は、当該鍵テーブルの第１行から順に行われ、最初に合致するまで照合が繰り返される。ここで、有効なアドレスとは図５に示すＶａｌｉｄビットが活性状態であるものである。例えばＶａｌｉｄビットが”１”の状態を活性状態とするならば、即ちＶａｌｉｄビットが”０”である行の情報は無効となる。例えばＭＡＣアドレス＃２のＶａｌｉｄビットが”０”であると、K_{2Even}、K_{2Odd}に何が設定されていてもこれらの値は参照されない。

ステップＳＰ８において否定結果が得られた場合、このことはＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在せず、当該パケットは受信装置２１が受信すべきパケットではないことを表しており、復号部３４はステップＳＰ１３に進み、当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

これに対してステップＳＰ８において肯定結果が得られた場合、このことはＭＲに合致するＭＡＣアドレスが鍵テーブル上に存在し、当該パケットは受信装置２１が受信すべきパケットであることを表しており、復号部３４はステップＳＰ９に進み、レジスタｋにＭＡＣアドレスが（１）式の条件下で合致した鍵の索引番号を代入し、ステップＳＰ１０へ進む。

ステップＳＰ１０において、復号部３４はＰＳＣの上位ビットに基づいて、当該パケットがＥｖｅｎ期間の鍵で暗号化されているのかＯｄｄ期間の鍵で暗号化されていのかを判断する。例えばＰＳＣの上位ビットが”０”の場合にＥｖｅｎ

期間、”１”の場合にＯｄｄ期間であると定める。

そして復号部３４は、ＰＳＣの上位ビットが”０”であった場合は、合致したＭＡＣアドレス＃ｉに対応するＥｖｅｎ期間の鍵及びK_{iEven}のＶａｌｉｄビットの値を鍵テーブルから取り出し、ＰＳＣの上位ビットが”１”であった場合は、合致したＭＡＣアドレス＃ｉに対応するＯｄｄ期間の鍵及びK_{iOdd}のＶａｌｉｄビットの値を鍵テーブルから取り出し、次のステップＳＰ１１に進む。

ステップＳＰ１１において、復号部３４は、取り出したＶａｌｉｄビットの値が、”１”であるか（すなわちＶａｌｉｄ（ｋ、ＥＯ）＝１）であるか否かを判断する。ステップＳＰ１１において否定結果が得られた場合、このことはＶａｌｉｄ（ｋ、ＥＯ）が”０”であること、すなわちパケットが暗号化されているにもかかわらず有効な復号鍵（個別鍵）が存在しないことを表しており、復号部３４はステップＳＰ１３に進んで当該パケットを破棄し、ステップＳＰ１４で処理を終了する。

これに対してステップＳＰ１１において肯定結果が得られた場合、このことはＶａｌｉｄ（ｋ、ＥＯ）が”１”であること、すなわちパケットに対する有効な復号鍵（個別鍵）が存在することを表しており、復号部３４はステップＳＰ１２に進む。

ステップＳＰ１２において復号部３４は、ＫＥＹ（ｋ、ＥＯ）すなわちｋ番めのＥＯに対応する復号鍵を鍵テーブル３７から取り出し、当該復号鍵を用いてパケットを復号して後段のチェッカ３５に出力し、ステップＳＰ１４で処理を終了する。

かくして復号部３４は、鍵テーブル３７及びハッシュテーブルに基づいて、ユニキャスト、マルチキャスト及びブロードキャストの各配信形態に対応したパケット復号処理を行う。

ここで、かかる復号処理における復号鍵の検索処理（ステップＳＰ５～ＳＰ１３）は、ＭＡＣアドレスの弁別処理（ステップＳＰ１～ＳＰ４）とは独立に処理されるため、ブロードキャストアドレスに対しても暗号化処理を行うことができ

る。この場合、共通鍵をブロードキャストアドレスに対する通信の復号鍵とする第１の方法と、ブロードキャストアドレスを個別鍵に対応するＭＡＣアドレスとして鍵テーブルへ登録する第２の方法の２つの共通鍵設定方法が考えられる。

第１の方法では、鍵テーブル３７の記憶領域は消費しないが他の同報通信と鍵を共用しなければならない。第２の方法では鍵テーブルの記憶領域を消費するものの、ブロードキャスト専用の復号鍵を設定することができる。

（１－５）実施の形態における動作及び効果

以上の構成において、復号部３４は、受信したデータストリームＤ３１の各パケットに記述されたＭＡＣアドレスに基づいて、ブロードキャストアドレス（”０ｘＦＦＦＦＦＦＦＦＦＦＦＦ”）を有するパケットを弁別するとともに、マスクビットを用いたＭＡＣアドレスの照合を行い、マルチキャスト及びユニキャストのパケットを弁別する。このとき復号部３４はＭＡＣアドレスのハッシュ値を算出し、当該ハッシュ値に基づいてマルチキャスト及びユニキャストのパケット弁別を行う。

そして復号部３４は、弁別されたパケットが暗号化されているかを検出し、当該パケットが暗号化されている場合、復号鍵を鍵テーブルより取り出して復号処理を行う。このとき復号部３４はパケットのＣＫＩに基づいて、当該パケットの暗号化が共通鍵によるものか個別鍵によるものかを判別し、これに応じて共通鍵又は個別鍵を用いてパケットを復号する。

以上の構成によれば、特定のＭＡＣアドレスをブロードキャストアドレスとして用いるとともに、マスクビットを用いてＭＡＣアドレスの一部のビットのみを照合するようにしたことにより、ブロードキャスト、マルチキャスト及びユニキャストといった様々な受信制御を行うことができる。

また、ハッシュ関数を用いてＭＡＣアドレスのビット数を縮小し、当該縮小したＭＡＣアドレスを用いてパケットの弁別を行うようにしたことにより、復号部３４の回路規模を縮小することができる。

（１－６）他の実施の形態

なお上述の実施の形態においては、マスクビットが”１”である位置のビットを、ＭＡＣアドレスの比較対象としたが、本発明はこれに限らず、逆にマスクビットが”０”である位置のビットをＭＡＣアドレスの比較対象とするようにしても良い。

また上述の実施の形態においては、ハッシュテーブルを用いたパケットの弁別において、ハッシュテーブルの検索結果が”０”である場合にパケットを破棄するようにしたが、本発明はこれに限らず、逆にハッシュテーブルの検索結果が”１”である場合にパケットを破棄するようにハッシュテーブルを設定しても良い。

さらに上述の実施の形態においては、ＭＡＣアドレス”０ｘＦＦＦＦＦＦＦＦＦＦＦＦ”をブロードキャストアドレスとしたが、本発明はこれに限らず、これ以外のＭＡＣアドレス”０ｘＦＦＦＦＦＦＦＦＦＦＦＦ”をブロードキャストアドレスとしても良い。

さらに上述の実施の形態においては、復号処理においてブロードキャストアドレスの弁別（ステップＳＰ２）、鍵テーブルにおけるＭＡＣアドレスの照合（ステップＳＰ３）、ハッシュテーブルの検索（ステップＳＰ４）の順で処理を行うようにしたが、本発明はこれに限らず、これ以外の順序で復号処理を行うようにしても良い。

さらに上述の実施の形態においては、衛星データ伝送システムに本発明を適用する場合について述べたが、本発明はこれに限らず、これ以外のデータ伝送システム、例えばケーブルインターネット等に適用しても良い。

（２）第２の実施の形態

図７は、本発明を適用した放送システム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一

実施の形態の構成例を示している。

図７の実施の形態においては、放送システムは、送信システム１０１、衛星１０２、受信システム１０３、およびネットワーク１０４から構成されている。なお、図７では、図が煩雑になるのを避けるため、１０１の受信システム（受信システム１０３）しか図示していないが、受信システムは、２以上設けることが可能である。

送信システム１０１は、制御装置１１１、データサーバ１１２、送信処理装置１１３、アンテナ１１４、回線接続装置１１５、およびケーブル１１６で構成され、制御装置１１１、データサーバ１１２、送信処理装置１１３、および回線接続装置１１５は、ケーブル１１６を介して相互に接続されることで、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を構成している。

制御装置１１１は、データサーバ１１２を制御することにより、送信処理装置１１３に対して、衛星放送で配信すべきデータを供給させる。また、制御装置１１１は、回線接続装置１１５を制御することにより、インターネット等の外部のネットワーク１０４から、衛星放送で配信すべきデータを取得させ、送信処理装置１１３に対して供給させる。さらに、制御装置１１１は、送信処理装置１１３における各種の処理を制御する。

データサーバ１１２は、衛星放送で配信すべきデータを記憶しており、制御装置１１１の制御にしたがって、必要なデータを、送信処理装置１１３に供給する。

送信処理装置１１３は、制御装置１１１の制御にしたがい、データサーバ１１２や回線接続装置１１５から供給されるデータを、例えば、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットにパケット化し、さらに、そのＩＰパケットを、ＤＶＢデータ放送仕様に準拠したセクション、即ち、例えば、ＥＮ　３０１　１９２　Ｖ１．１．１（１９９７－１２）、ＤＶＢ　ｓｐｅｃｉｆｉｃａｔｉｏｎ　ｆｏｒ　ｄａｔａ　ｂｒｏａｄｃａｓｔｉｎｇ　ＥＴＳＩ（Ｅｕｒｏｐｅａｎ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｔａｎｄ－

ａｒｄｓ　Ｉｎｓｔｉｔｕｔｅ）で規定されているマルチプロトコルエンキャプスレイション（Ｍｕｌｔｉｐｒｏｔｏｃｏｌ　Ｅｎｃａｐｓｕｌａｔｉｏｎ）に基づくディスクリプタで記述されたセクションと呼ばれるデータブロックにブロック化する。そして、送信処理装置１１３は、セクションを、所定長のペイロードに分割し、各ペイロードに、ＭＰＥＧ２のトランスポートストリームを構成するパケット（以下、適宜、ＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）パケットという）のヘッダを付加することで、ＴＳパケットに類するパケットを構成し、さらに、変調、増幅等の必要な処理を施して、アンテナ１１４から、衛星放送波として送出する。

また、送信処理装置１１３は、受信システム１０３を構成する端末124_1，124_2，・・・（図７において図示していない受信システムを構成する端末についても同様）それぞれのＭＡＣアドレスと、各ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスに割り当てた暗号鍵とを対応付けた表形式の暗号鍵テーブルを記憶している暗号鍵テーブル記憶部１１３Ａを有している。なお、各ＭＡＣアドレスに割り当てる暗号鍵は、基本的には、すべて異なるものとする。但し、一部のＭＡＣアドレスについて、同一の暗号鍵を割り当てるようにしても良い。

ここで、ＭＡＣアドレスとは、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｅｌｅｃｔｒｉｃａｌ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｅｎｇｉｎｅｅｒｓ）８０２．３等に適用されるアドレス体系であり、通信ポートごとに固有の４８ビットの値で、重複がないことが保証されている。４８ビットのＭＡＣアドレスは、その上位２４ビットが、ＩＥＥＥによって登録／管理される製造者（ベンダ（ｖｅｎｄｏｒ））識別番号となっており、その下位２４ビットが、各ベンダによって管理される機器識別番号となっている。ＭＡＣアドレスによれば、受信システム１０３の各端末124_i（ｉ＝１，２，・・・）を特定することができる。

上述のマルチプロトコルエンキャプスレイションによれば、セクションのヘッダ（セクションヘッダ）には、そのセクションのペイロードに配置されたデータ

を配信する端末２４_{i}の宛先として、その端末のＭＡＣアドレスが配置されるようになっている。セクションのペイロードに配置されるデータ、即ち、ここでは、ＩＰパケットを暗号化する必要がある場合には、送信処理装置１１３は、セクションのヘッダに配置される宛先としての、端末１２４_{i}のＭＡＣアドレスに割り当てられた暗号鍵を、暗号鍵テーブル記憶部１１３Ａに記憶された暗号鍵テーブルから読み出し、その暗号鍵で、そのセクションのペイロードに配置されるＩＰパケットを暗号化するようになっている。

なお、暗号鍵テーブルは、受信システム１０３を構成する、後述する受信装置１２２が有する鍵テーブルと同一形式のものであっても良いし、異なる形式のものであっても良い。また、ここでは、暗号鍵テーブルを、送信システム１０１に内蔵させておくようにしたが、暗号鍵テーブルは、例えば、ネットワーク１０４上の図示せぬサーバに記憶させておき、必要に応じて、回線接続装置１１５を介して読み出して使用するようにすることも可能である。

回線接続装置１１５は、例えば、モデムや、ＴＡ（Ｔｅｒｍｉｎａｌ　Ａ－ｄａｐｔｅｒ）およびＤＳＵ（Ｄｉｇｉｔａｌ　Ｓｅｒｖｉｃｅ　Ｕｎｉｔ）等で構成され、ネットワーク１０４を介しての通信制御を行うようになっている。

受信システム１０３は、アンテナ１２１、受信装置１２２、回線接続装置１２３、端末１２４_{1}，１２４_{2}，・・・、およびケーブル１２５で構成されており、受信装置１２２、回線接続装置１２３、端末１２４_{1}，１２４_{2}，・・・は、ケーブル１２５を介して相互に接続され、これにより、例えば、イーサネット（商標）等のＬＡＮを構成している。

なお、受信装置１２２や、端末１２４_{1}，１２４_{2}，・・・は、例えば、コンピュータで構成することができる。

また、ここでは、受信装置１２２と、端末１２４_{1}，１２４_{2}，・・・とは、ケーブル１２５で相互に接続することにより、ＬＡＮを構成させるようにしたが、受信装置１２２と、端末１２４_{1}，１２４_{2}，・・・とは、直接接続するようにすることも可能である。

さらに、受信装置１２２は、１台の端末１２４$_i$としてのコンピュータのスロットに装着可能なボードとして構成することが可能である。

また、受信装置１２２と回線接続装置１２３とは、１台のコンピュータで構成することが可能である。

衛星１０２を介して、送信システム１０１から送信されてくる衛星放送波は、アンテナ１２１で受信され、その受信信号は、受信装置１２２に供給される。受信装置１２２は、アンテナ１２１からの受信信号に対して、後述するような処理を施し、その結果得られるデータを、所定の端末１２４$_i$に供給する。

回線接続装置１２３は、回線接続装置１１５と同様に構成され、ネットワーク１０４を介しての通信制御を行うようになっている。

端末１２４$_1$，１２４$_2$，・・・は、例えば、コンピュータで構成され、受信装置１２２から必要なデータを受信して、表示、出力、あるいは記憶等するようになっている。

次に、図８のフローチャートを参照して、送信システム１０１が行うデータの送信処理について説明する。

まず最初に、ステップＳＰ１０１において、制御装置１１１は、端末１２４$_i$に対して送信すべきデータがあるかどうかを判定する。

ここで、制御装置１１１は、データを送信するスケジュールが記述されたスケジュール表を有しており、そのスケジュール表に基づいて、端末１２４$_i$に対して送信すべきデータがあるかどうかを判定する。また、端末１２４$_i$は、回線接続装置１２３を制御することにより、ネットワーク１０４を介して、送信システム１０１に対して、データを要求することができるようになっており、制御装置１１１は、そのような要求が、ネットワーク１０４を介して回線接続装置１１５で受信されたかどうかによって、端末１２４$_i$に対して送信すべきデータがあるかどうかを判定する。

ステップＳＰ１０１において、端末１２４$_1$に対して送信すべきデータがないと判定された場合、ステップＳＰ１０２に進み、制御装置１１１は、期間を変更

するかどうかを判定する。

ここで、送信システム１０１においては、暗号鍵テーブル記憶部１１３における暗号鍵テーブルに記述された暗号鍵が、定期的または不定期に更新されるようになっており、例えば、偶数回目の更新によって得られた暗号鍵を用いて暗号化が行われる期間が、Ｅｖｅｎ期間と呼ばれ、奇数回目の更新によって得られた暗号化器を用いて暗号化が行われる期間が、Ｏｄｄ期間と呼ばれる。従って、Ｅｖｅｎ期間とＯｄｄ期間とは交互に現れるが、ステップＳ２では、Ｅｖｅｎ期間からＯｄｄ期間に、またはＯｄｄ期間からＥｖｅｎ期間に変更する時期であるかどうかが判定される。

ステップＳＰ１０２において、期間を変更しないと判定された場合、即ち、いま暗号化に用いている暗号鍵をそのまま用いて、データの暗号化を続行する場合、ステップＳＰ１０１に戻り、以下、上述の場合と同様の処理を繰り返す。

また、ステップＳＰ１０２において、期間を変更すると判定された場合、即ち、いまが、Ｅｖｅｎ期間であるときにはＯｄｄ期間に、Ｏｄｄ期間であるときにはＥｖｅｎ期間に、期間を変更する場合、ステップＳＰ１０３に進み、制御装置１１１は、暗号鍵テーブルに記憶された暗号鍵を、後述するステップＳＰ１０４において前回生成された暗号鍵に更新し、これにより、その後は、送信処理装置１１３において、その更新された暗号鍵を用いて暗号化が行われる。

そして、ステップＳＰ１０４に進み、制御装置１１１は、次の期間に用いる暗号鍵を生成し（あるいは取得し）、送信処理装置１１３に供給して、復号鍵として送信させ、ステップＳＰ１０１に戻り、以下、上述の場合と同様の処理が繰り返される。なお、復号鍵の送信は、衛星１０２を介して行う他、ネットワーク１０４を介して行うことも可能である。

即ち、次の期間に用いる新たな復号鍵を、その、次の期間の開始直前に、受信システム１０３に送信したのでは、受信システム１０３において、新たな復号鍵の設定が、次の期間の開始までに間に合わないことがある。そこで、本実施の形態では、次の期間に用いる新たな暗号鍵は、その直前の期間において、受信シス

テム１０３に対して配信されるようになっている。

一方、ステップＳＰ１０１において、端末１２４$_i$に対して送信すべきデータがあると判定された場合、制御装置１１１は、データサーバ１１２または回線接続装置１１５を制御することにより、その送信すべきデータを、送信処理装置１１３に供給させる。送信処理装置１１３は、データサーバ１１２または回線接続装置１１５から供給されるデータを受信し、ＩＰパケットにパケット化して、ステップＳＰ１０５に進む。

送信処理装置１１３は、ステップＳＰ１０５において、ＩＰパケットが、暗号化の必要なものであるかどうかを判定し、暗号化の必要なものでないと判定した場合、ステップＳＰ１０６およびＳＰ１０７をスキップして、ステップＳＰ１０８に進む。

また、ステップＳＰ１０５において、ＩＰパケットが、暗号化の必要なものであると判定された場合、ステップＳＰ１０６に進み、送信処理装置１１３は、そのＩＰパケットの宛先となる端末１２４$_i$のＭＡＣアドレスに割り当てられた暗号鍵を、暗号鍵テーブルから読み出し、ステップＳＰ１０７に進む。ステップＳＰ１０７では、送信処理装置１１３は、ＩＰパケットを、ステップＳＰ１０６で読み出した暗号鍵で暗号化し、ステップＳＰ１０８に進む。

ステップＳＰ１０８では、送信処理装置は、ＩＰパケットについてＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋｉｎｇ）コード（あるいは、チェックサム）を演算し、そのＩＰパケットをペイロードとして、その最後に、ＣＲＣコードを配置するとともに、その先頭に、セクションヘッダを配置することで、図９（Ａ）に示すようなセクションを構成する。なお、ペイロードとＣＲＣコードとの間には、必要に応じて、スタッフィングバイトが挿入される。

セクションヘッダは、図９（Ｂ）に示すように、３バイト（９６ビット）で構成される。ここで、セクションヘッダの詳細については、上述のＥＮ　３０１１９２　Ｖ１．１．１（１９９７－１２）に記載されているため、その説明は省略するが、図９（Ｂ）におけるＭＡＣ　ａｄｄｒｅｓｓ１乃至６に、宛先となる

４８ビットのＭＡＣアドレスが配置される。ここで、ＭＡＣ　ａｄｄｒｅｓｓ　１には、ＭＡＣアドレスの最上位ビットから８ビットが配置され、ＭＡＣ　ａｄｄｒｅｓｓ　２には、その次の上位８ビットが配置される。そして、ＭＡＣ　ａｄｄｒｅｓｓ　３乃至５それぞれに、同様にしてＭＡＣアドレスが８ビットずつ配置され、ＭＡＣ　ａｄｄｒｅｓｓ　６には、ＭＡＣアドレスの最下位の８ビットが配置される。

送信処理装置１１３は、セクションを構成した後、そのセクションを、所定長のペイロードに分割し、各ペイロードに、ＭＰＥＧ２のトランスポートストリームを構成するＴＳパケットのヘッダを付加することで、ＴＳパケットに類するパケットを構成するカプセル化を行う。そして、送信処理装置１１３は、ステップＳＰ１０９に進み、その結果得られるパケット（このパケットは、基本的には、ＴＳパケットと同様に処理することができるので、以下、適宜、ＴＳパケットという）に対して、変調、増幅等の必要な処理を施して、アンテナ１１４から、衛星放送波として送出し、ステップＳＰ１０１に戻る。

なお、図９（Ｂ）に示したセクションヘッダにおいて、その先頭から４３ビット目と４４ビット目の２ビットに配置される２ビットのＰＳＣ（ｐａｙｌｏａｄ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌ）は、例えば、セクションのペイロードに配置されたデータが暗号化されているかどうかを表す暗号化判定フラグ、およびそのデータが、Ｅｖｅｎ期間またはＯｄｄ期間のうちのいずれの期間のものかを表す期間判定フラグとして用いられるようになっている。

具体的には、例えば、ＰＳＣの下位ビットは、暗号化判定フラグとして用いられ、データが暗号化されているときには１に、暗号化されていないときには０とされる。また、ＰＳＣの上位ビットは、期間判定フラグとして用いられ、Ｅｖｅｎ期間では０に、Ｏｄｄ期間では１にされる。但し、ＰＳＣの上位ビットを、暗号化判定フラグとして用いるとともに、その下位ビットを、期間判定フラグとして用いることも可能である。また、暗号化判定フラグの０と１の割り当てや、期間判定フラグの０と１の割り当ては、上述した場合と逆にすることも可能である

。

ここで、ＤＶＢの規格であるＥＮ　３０１　１９２　Ｖ１．１．１（１９９７－１２）では、ＰＳＣが、００Ｂ（Ｂは、その前に配置された値が２進数であることを表す）の場合が、データが暗号化されていないことを表すこととなっており、従って、暗号化判定フラグは、データが暗号化されているときには１に、暗号化されていないときには０とする方が、ＤＶＢの規格に反しないこととなるので望ましい。

以上のように、図７の放送システムでは、各端末１２４$_i$に固有のＭＡＣアドレスに割り当てられた暗号鍵で、データが暗号化されるので、各端末１２４$_i$ごとの受信制御という、いわば究極の限定受信機構を実現することができる。

なお、ＭＡＣアドレス、あるいはＩＰアドレス等の受信側に固有の値に暗号鍵を割り当てて、きめ細かい受信制御を行う限定受信機構を実現する方法については、本件出願人が先に提案した、例えば、特開平１０－２１５２４４号公報に、その詳細が開示されている。但し、わが国における通信衛星放送が、ＤＶＢ－ＳＩ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｂｒｏａｄｃａｓｔｉｎｇ－Ｓｅｒｖｉｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ／ＥＮ３００－４６８）から派生した仕様に準拠している現状においては、上述したように、ＭＡＣアドレスを用いるのが、その仕様に適合することとなる。

次に、図１０は、図７の受信装置１２２の構成例を示している。

アンテナ１２１は、衛星１０２を介して、送信システム１０１から送信されてくる衛星放送波を受信し、その受信信号を、フロントエンド部１３１に出力する。フロントエンド部１３１は、ＣＰＵ１３４の制御にしたがい、アンテナ１２１からの受信信号から所定のチャンネルの信号を選局し、さらに、その信号を、ＴＳパケットのディジタルストリーム（ＩＰ__ｄａｔａｇｒａｍ__ｄａｔａ__ｂｙｔｅ）に復調して、デマルチプレクサ１３２に出力する。デマルチプレクサ１３２は、ＣＰＵ１３４の制御にしたがい、フロントエンド部１３１からのディジタルストリームから、所定のＴＳパケットを抽出し、復号ＬＳＩ（Ｌａｒｇｅ

Ｓｃａｌｅ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）１３３に出力する。即ち、デマルチプレクサ１３２は、フロントエンド部１３１からのディジタルストリームを構成するＴＳパケットのヘッダに配置されているＰＩＤ（Ｐａｃｋｅｔ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）に基づいて、ＴＳパケットの取捨選択を行い、選択したＴＳパケットのみを、復号ＬＳＩ１３３に出力する。

復号ＬＳＩ１３３は、１チップのＬＳＩで、フィルタ１４１、復号器１４２、鍵テーブル記憶部１４３、チェッカ１４４、およびＦＩＦＯ（Ｆｉｒｓｔ Ｉｎ Ｆｉｒｓｔ Ｏｕｔ）バッファ１４５で構成されている。

フィルタ１４１は、ＣＰＵ１３４の制御にしたがい、デマルチプレクサ１３２からのＴＳパケットで構成されるセクションのペイロードに配置されたデータを、必要に応じて検査し、不必要なＴＳパケットを破棄し、必要なＴＳパケットだけを復号器１４２に出力する。

復号器１４２は、フィルタ１４１からのＴＳパケットで構成されるセクションのペイロードに配置されたデータ（ここでは、ＩＰパケット）を、鍵テーブル記憶部１４３に記憶された復号鍵で復号し、チェッカ１４４に出力する。また、復号器１４２は、図８で説明したように、送信システム１０１において暗号鍵が更新され、その更新された暗号鍵が送信されてきた場合、ＣＰＵ１３４の制御にしたがい、その暗号鍵を、復号鍵として、鍵テーブル記憶部１４３の記憶内容を更新する。従って、ここでは、暗号化方式として、共通鍵暗号化方式が用いられるようになっている。但し、暗号化方式としては、公開鍵暗号化方式を用いることも可能である。

鍵テーブル記憶部１４３は、受信装置１２２にケーブル１２５を介して接続された端末124_1，124_2，・・・それぞれのＭＡＣアドレスと、それぞれに割り当てられた復号鍵とが対応付けられて登録された鍵テーブルを記憶している。

チェッカ１４４は、ＣＰＵ１３４の制御にしたがい、復号器１４２が出力するＩＰパケットについて、そのＩＰパケットが配置されていたセクションのＣＲＣコードを用いて誤り検出を行い、これにより、復号器１４２における復号が正常

に行われたかどうか等を判定する。チェッカ１４４で処理されたＩＰパケットは、ＦＩＦＯバッファ１４５に供給されるようになっており、ＦＩＦＯバッファ１４５は、チェッカ１４４からのＩＰパケットを一時記憶し、ＣＰＵ１３４の制御にしたがい、記憶したＩＰパケットを、Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）１３５に出力する。これにより、ＩＰパケットのデータレートが調整される。

ＣＰＵ１３４は、フロントエンド部１３１、デマルチプレクサ１３２、復号ＬＳＩ１３３、およびＩ／Ｆ１３５を制御する。Ｉ／Ｆ１３５は、ＣＰＵ１３４の制御にしたがい、ＦＩＦＯバッファ１４５からのＩＰパケットを、ケーブル１２５を介して、端末124_iに供給するインタフェースとして機能する。

次に、図１１は、図１０の鍵テーブル記憶部１４３に記憶されている鍵テーブルの構成例を示している。

鍵テーブルは、例えば、ケーブル１２５に接続されている端末124_1，124_2，・・・の数と同一数のエントリから構成されている。図１１では、鍵テーブルは、Ｎ個のエントリ＃１乃至＃Ｎを有しており、従って、本実施の形態では、ケーブル１２５には、Ｎ個の端末124_1乃至124_Nが接続されている。なお、鍵テーブルのエントリの最大数は、鍵テーブル記憶部１４３の記憶容量等によって制限される。

各エントリ＃ｉ（Ｉ＝１，２，・・・，Ｎ）には、端末124_iの４８ビットのＭＡＣアドレスＭＡＣａｄｄｒｅｓｓ＃ｉと、そのＭＡＣアドレスに割り当てられたｍビットの復号鍵（ｍは、使用する暗号形式による）とが対応付けられて登録されている。なお、本実施の形態では、上述したように、Ｅｖｅｎ期間とＯｄｄ期間とが存在し、それぞれの期間では、異なる暗号鍵で暗号化が行われるため、各エントリ＃ｉには、Ｅｖｅｎ期間に暗号化されたデータを復号するための復号鍵（以下、適宜、Ｅｖｅｎ復号鍵という）$K_{Even\#i}$と、Ｏｄｄ期間に暗号化されたデータを復号するための復号鍵（以下、適宜、Ｏｄｄ復号鍵という）$K_{Odd\#i}$との２つの復号鍵が登録されている。

さらに、各エントリ＃ｉのＭＡＣアドレスＭＡＣａｄｄｒｅｓｓ＃ｉの先頭に

は、そのエントリ＃ｉが有効であるかどうかを表すＶａｌｉｄビット（以下、適宜、エントリＶａｌｉｄビットという）が付加されている。また、各エントリ＃ｉのＥｖｅｎ復号鍵$K_{Even\#i}$とＯｄｄ復号鍵$K_{Odd\#i}$にも、それぞれが有効かどうかを表すＶａｌｉｄビット（以下、適宜、復号鍵Ｖａｌｉｄビットという）が付加されている。

ここで、エントリＶａｌｉｄビット、復号鍵Ｖａｌｉｄビットは、例えば、それが１の場合が有効であることを表し、０の場合が有効でないことを表す。但し、エントリＶａｌｉｄビット、復号鍵Ｖａｌｉｄビットの０と１の割り当ては、上述した場合と逆にすることも可能である。

上述したように、送信システム１０１においては、次の期間に用いる新たな暗号鍵と同一の復号鍵は、その直前の期間に、受信システム１０３に対して配信されるようになっている。従って、Ｅｖｅｎ期間においては、その次のＯｄｄ期間で用いられる暗号鍵と同一の復号鍵（Ｏｄｄ復号鍵）が配信され、Ｏｄｄ期間においては、その次のＥｖｅｎ期間で用いられる暗号鍵と同一の復号鍵（Ｅｖｅｎ復号鍵）が配信される。そして、復号器１４２では、ＣＰＵ１３４の制御の下、そのようにして配信されてくる復号鍵が、鍵テーブルに設定（例えば、上書き）される。従って、この場合、鍵テーブルには、次の期間に用いられる復号鍵が、現在の期間が終了するまでに設定され、さらに、期間の変更に伴う復号鍵の変更は、ＣＰＵ１３４を介在せずに、復号器１４２が読み出しを行う鍵テーブルの位置（アドレス）を切り替えるだけで済むので、瞬時に行うことができる。

次に、図１２のフローチャートを参照して、図１０の受信装置１２２の動作について説明する。

アンテナ１２１では、衛星１０２を介して、送信システム１０１から送信されてくる衛星放送波が受信され、その結果得られる受信信号は、フロントエンド部１３１およびデマルチプレクサ１３２を介することにより、ＴＳパケットのディジタルストリームとされ、復号ＬＳＩ１３３に供給される。

復号ＬＳＩ１３３では、デマルチプレクサ１３２が出力するＴＳパケットで構

成されるセクションが、フィルタ１４１を介して、復号器１４２に供給される。復号器１４２は、セクションを受信し、ステップＳＰ１１１において、そのセクションヘッダに配置されたＭＡＣアドレスを、内蔵するレジスタとしての変数ＭＡにセットする。

復号器１４２は、鍵テーブルを参照することにより、変数ＭＡに一致するＭＡＣアドレスのエントリを検索し、即ち、鍵テーブルのエントリ＃１から順に、各エントリ＃ｉに登録されているＭＡＣアドレスを読み出して、そのＭＡＣアドレスと、変数ＭＡとを比較（照合）し、ステップＳＰ１１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在するかどうかを判定する。ステップＳＰ１１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在しないと判定された場合、即ち、セクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル１２５上に接続されていない場合、ステップＳＰ１１３に進み、復号器１４２は、そこに供給されたセクションを破棄し、処理を終了する。

また、ステップＳＰ１１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在すると判定された場合、そのエントリを注目エントリとして、ステップＳＰ１１４に進む。

ステップＳＰ１１４では、復号器１４２は、注目エントリのエントリＶａｌｉｄビットに基づいて、その注目エントリが有効であるかどうかを判定する。ステップＳＰ１１４において、注目エントリが有効でないと判定された場合、即ち、注目エントリのエントリＶａｌｉｄビットが０である場合、ステップＳＰ１１３に進み、復号器１４２は、そこに供給されたセクションを破棄し、処理を終了する。

従って、復号器１４２に供給されたセクションのセクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル１２５上に接続されている場合でも、そのＭＡＣアドレスのエントリが有効とされていないときには、そのセクションは、ケーブル１２５上の端末に供給されない。

また、ステップＳＰ１１４において、注目エントリが有効であると判定された

場合、即ち、注目エントリのエントリＶａｌｉｄビットが１である場合、ステップＳＰ１１５に進み、復号器１４２は、セクションヘッダのＰＳＣ（図９（Ｂ））の下位ビット、即ち、暗号化判定フラグを参照し、セクションのペイロードのデータ（ＩＰパケット）が暗号化されているかどうかを判定する。ステップＳＰ１１５において、暗号化判定フラグが０であると判定された場合、即ち、セクションのペイロードに配置されたＩＰパケットが暗号化されていない場合、ステップＳＰ１１７およびＳＰ１１８をスキップして、ステップＳＰ１１９に進み、復号器１４２は、その暗号化されていないＩＰパケットを、チェッカ１４４を介して、ＦＩＦＯバッファ１４５に出力して、処理を終了する。

そして、ＦＩＦＯバッファ１４５に記憶されたＩＰパケットは、Ｉ／Ｆ１３５を介して、そのＩＰパケットが配置されていたセクションのセクションヘッダにおけるＭＡＣアドレスによって特定されるケーブル１２５上の端末124_iに供給される。

一方、ステップＳＰ１１５において、暗号化判定フラグが１であると判定された場合、即ち、セクションのペイロードに配置されたＩＰパケットが暗号化されている場合、ステップＳＰ１１６に進み、復号器１４２は、そのセクションのセクションヘッダのＰＳＣ（図９（Ｂ））の上位ビット、即ち、期間判定フラグを、内蔵するレジスタとしての変数ＥＯにセットして、ステップＳＰ１１７に進む。

ステップＳＰ１１７では、復号器１４２は、ＭＡＣアドレスが変数ＭＡに一致する注目エントリにおける変数ＥＯに対応する期間、即ち、変数ＥＯが０である場合にはＥｖｅｎ期間、１である場合にはＯｄｄ期間の復号鍵の復号鍵Ｖａｌｉｄビット＃（ＭＡ，ＥＯ）が有効であるかどうかを判定する。ステップＳＰ１１７において、復号鍵Ｖａｌｉｄビット＃（ＭＡ，ＥＯ）が有効でないと判定された場合、即ち、復号鍵Ｖａｌｉｄビット＃（ＭＡ，ＥＯ）が０である場合、ステップＳＰ１１３に進み、復号器１４２は、そこに供給されたセクションを破棄し、処理を終了する。

従って、復号器１４２に供給されたセクションのセクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル１２５上に接続されており、そのＭＡＣアドレスのエントリが有効とされている場合でも、期間判定フラグが表す期間の復号鍵が有効とされていないときには、そのセクションは、ケーブル１２５上の端末に供給されない。

一方、ステップＳＰ１１７において、復号鍵Ｖａｌｉｄフラグ＃（ＭＡ，ＥＯ）が有効であると判定された場合、即ち、復号鍵Ｖａｌｉｄビット＃（ＭＡ，ＥＯ）が１である場合、ステップＳＰ１１８に進み、復号器１４２は、ＭＡＣアドレスが変数ＭＡに一致する注目エントリにおける、変数ＥＯに対応する期間の復号鍵Ｋｅｙ（ＭＡ，ＥＯ）を、鍵テーブルから読み出し、その復号鍵Ｋｅｙ（ＭＡ，ＥＯ）で、セクションのペイロードに配置されたＩＰパケットを復号し、ステップＳＰ１１９に進む。

ステップＳＰ１１９では、復号器１４２は、復号されたＩＰパケットを、チェッカ１４４を介して、ＦＩＦＯバッファ１４５に出力して、処理を終了する。

そして、ＦＩＦＯバッファ１４５に記憶されたＩＰパケットは、Ｉ／Ｆ１３５を介して、そのＩＰパケットが配置されていたセクションのセクションヘッダにおけるＭＡＣアドレスによって特定されるケーブル１２５上の端末124_iに供給される。

なお、図１２のフローチャートにしたがった処理は、復号器１４２に対して、セクションが供給されるごとに行われる。

以上のように、鍵テーブルのエントリに登録されたエントリＶａｌｉｄビットに基づいて、そのエントリが有効かどうかを判定し、端末に対するデータの出力を制御するようにしたので、データを正常に取得する（受信する）ことのできるユーザ（端末）を、容易に制限することが可能となる。

さらに、鍵テーブルの復号鍵Ｖａｌｉｄビットにも基づいて、データの出力を制御するようにしたので、例えば、ある端末について、Ｅｖｅｎ期間またはＯｄｄ期間のうちのいずれか一方の期間のみのデータの受信を許可し、他方の期間の

データの受信を禁止することを、容易に行うことができる。

なお、エントリＶａｌｉｄビットおよび復号鍵Ｖａｌｉｄビットの設定は、受信装置１２２において、いわば自主的に行うことも可能であるし、また、送信システム１０１から送信されてくる情報に基づいて行うことも可能である。

また、本実施の形態では、復号鍵を（暗号鍵も）、端末に固有のＭＡＣアドレスに割り当てるようにしたが、復号鍵は、その他、例えば、端末に固有の端末ＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）を設定し、その端末ＩＤに割り当てるようにすることも可能である。さらに、復号鍵は、複数の端末ごとに固有のグループＩＤを設定し、そのグループＩＤごとに割り当てるようにすることも可能である。但し、ＭＡＣアドレスに対して復号鍵を割り当てる場合には、上述したようなきめの細かい限定受信機構を、ＤＶＢの規格であるＥＮ　３０１　１９２　Ｖ１．１．１（１９９７－１２）に準拠したディジタル衛星放送の枠組みに、容易に組み込むことが可能となる。

また、本実施の形態では、フィルタ１４１、復号器１４２、鍵テーブル記憶部１４３、チェッカ１４４、およびＦＩＦＯバッファ１４５を、１チップの復号ＬＳＩ１３３で構成するようにしたが、フィルタ１４１、復号器１４２、鍵テーブル記憶部１４３、チェッカ１４４、およびＦＩＦＯバッファ１４５は、それぞれ別のチップとして構成することも可能である。但し、フィルタ１４１、復号器１４２、鍵テーブル記憶部１４３、チェッカ１４４、およびＦＩＦＯバッファ１４５を、１チップの復号ＬＳＩ１３３で構成した方が、データの復号が、復号ＬＳＩ１３３の外部から完全に隠蔽された形で行われるため、セキュリティを向上させることができる。さらに、回路の実装面積の縮小や、処理の高速化等の観点からも、フィルタ１４１、復号器１４２、鍵テーブル記憶部１４３、チェッカ１４４、およびＦＩＦＯバッファ１４５は、１チップの復号ＬＳＩ１３３で構成するのが望ましい。

また、本実施の形態では、ディジタル衛星放送によってデータを配信する場合について説明したが、本発明は、その他、例えば、マルチキャストでデータを配

信する場合等にも適用可能である。

さらに、本実施の形態では、Ｅｖｅｎ期間とＯｄｄ期間の２つの期間を設けるようにしたが、そのような期間を設けないようにすることも可能であるし、３以上の期間を設けるようにすることも可能である。同様に、鍵テーブルの各エントリに登録する復号鍵の数も、１つだけとしたり、３以上とすることが可能である。

また、本実施の形態では、データを、ＤＶＢの規格に準拠する形で配信するようにしたが、データの配信は、ＤＶＢの規格に準拠しない形で行うことも可能である。

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや、１チップのマイクロコンピュータ等にインストールされる。

そこで、図１３は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク２０５やＲＯＭ２０３に予め記録しておくことができる。

あるいはまた、プログラムは、フロッピーディスク、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＭＯ（Ｍａｇｎｅｔｏ ｏｐｔｉｃａｌ）ディスク、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体２１１に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体２１１は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体２１１からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ（Ｌｏｃａｌ

Ａｒｅａ　Ｎｅｔｗｏｒｋ)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部２０８で受信し、内蔵するハードディスク２０５にインストールすることができる。

コンピュータは、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２０２を内蔵している。ＣＰＵ２０２には、バス２０１を介して、入出力インタフェース２１０が接続されており、ＣＰＵ２０２は、入出力インタフェース２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部２０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２０３に格納されているプログラムを実行する。あるいは、また、ＣＰＵ２０２は、ハードディスク２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部２０８で受信されてハードディスク２０５にインストールされたプログラム、またはドライブ２０９に装着されたリムーバブル記録媒体２１１から読み出されてハードディスク２０５にインストールされたプログラムを、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２０４にロードして実行する。これにより、ＣＰＵ２０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース２１０を介して、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）やスピーカ等で構成される出力部２０６から出力、あるいは、通信部２０８から送信、さらには、ハードディスク２０５に記録等させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１のコンピュータにより処理されるものであっても良い

し、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

産業上の利用の可能性

本発明は、ディジタル衛星放送を介したデータ伝送システムや、有線ネットワークを介したデータ伝送システムに利用することができる。

請 求 の 範 囲

1．送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送システムにおいて、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する上記送信装置と、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する上記受信装置と

を具えることを特徴とする情報伝送システム。

2．上記送信装置は、上記複数の上記受信装置全てにデータを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信し、

上記受信装置は、受信した上記データに上記同報アドレスが付せられているとき、当該データを復号する

ことを特徴とする請求の範囲第1項に記載の情報伝送システム。

3．上記受信装置は、上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行う

ことを特徴とする請求の範囲第1項に記載の情報伝送システム。

４．上記送信装置は、上記受信装置に対して個別にデータを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化し、

上記受信装置は、当該受信装置に対して個別に送信されたデータを、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて復号するとともに、任意のグループの上記受信装置間に対して送信されたデータを、上記共通鍵を用いて復号する

ことを特徴とする請求の範囲第１項に記載の情報伝送システム。

５．送信装置から所定の伝送路を介して、それぞれ固有のアドレスを有する複数の受信装置にデータを伝送する情報伝送方法において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアドレスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する送信ステップと、

上記データを受信し、固有の上記アドレスと当該データに付せられた上記アドレスとが一致したとき、又は固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する受信ステップと

を具えることを特徴とする情報伝送方法。

６．それぞれ固有のアドレスを有する複数の受信装置にデータを送信する送信装置において、

上記受信装置に対して個別にデータを送信するとき、当該受信装置固有のアド

レスを当該データに付して送信するとともに、任意のグループの上記受信装置に対して共通のデータを送信するとき、上記任意のグループの上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と、当該アドレスの共通部分の範囲を指定するアドレス範囲情報とを当該データに付して送信する

ことを特徴とする送信装置。

7．上記複数の上記受信装置全てに上記データを送信するとき、所定の同報アドレスを上記共通アドレス情報として上記データに付して送信する

ことを特徴とする請求の範囲第6項に記載の送信装置。

8．上記受信装置に対して個別に上記データを送信するとき、当該受信装置固有の上記アドレスに対応した秘密鍵を用いて当該データを暗号化するとともに、任意のグループの上記受信装置間に対して共通のデータを送信するとき、所定の共通鍵を用いて当該データを暗号化する

ことを特徴とする請求の範囲第6項に記載の送信装置。

9．所定の送信装置から送信されたデータを受信して復号する受信装置において、

受信した上記データに付せられたアドレスと、当該受信装置固有のアドレスとが一致したとき、又は、受信した上記データに付せられた、複数の上記受信装置間で共通する上記アドレスの共通部分を表す共通アドレス情報と当該アドレスの共通部分の範囲を指定するアドレス範囲情報とに基づいて、固有の上記アドレスと当該データに付せられた上記共通アドレス情報とを上記アドレス範囲情報が示す範囲で比較して比較結果が一致したとき、上記データを復号する

ことを特徴とする受信装置。

10．受信した上記データに所定の同報アドレスが付せられているとき、当該デ

ータを復号する

ことを特徴とする請求の範囲第９項に記載の受信装置。

１１．上記アドレスをより少ないビット数のアドレスに変換し、当該変換したアドレスを用いて、固有の上記アドレスと上記データに付せられた上記アドレスとの比較を行う

ことを特徴とする請求の範囲第９項に記載の受信装置。

１２．データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理装置であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、

上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定手段と、

上記判定手段による判定結果に基づいて、上記データブロックに配置されたデータの出力を制御する出力制御手段と

を備えることを特徴とするデータ処理装置。

１３．上記出力制御手段は、

上記注目エントリが有効である場合に、上記データを、上記データブロックに配置された宛先に出力し、

上記注目エントリが有効でない場合に、上記データを破棄する

ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

１４．上記データは暗号化されており、

その暗号化されたデータを復号する復号手段をさらに備える
ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

１５．上記データは、そのデータの宛先に割り当てられた鍵を用いて暗号化されており、
上記テーブルの各エントリには、上記宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されており、
上記復号手段は、上記テーブルに登録されている上記鍵を用いて、上記データを復号する
ことを特徴とする請求の範囲第１４項に記載のデータ処理装置。

１６．上記復号手段は、上記テーブルの、上記データブロックの宛先に割り当てられた上記鍵を用いて、そのデータブロックに配置されたデータを復号する
ことを特徴とする請求の範囲第１５項に記載のデータ処理装置。

１７．上記テーブルの各エントリには、上記宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されており、
上記復号手段は、
上記データブロックの宛先に割り当てられた上記鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定し、
有効である場合に、上記鍵を用いて、データを復号する
ことを特徴とする請求の範囲第１６項に記載のデータ処理装置。

１８．上記テーブルの各エントリには、上記宛先およびエントリ有効情報の他、その宛先に割り当てられた２以上の鍵が登録されている
ことを特徴とする請求の範囲第１５項に記載のデータ処理装置。

１９．上記テーブルの各エントリには、上記２以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報が登録されている
ことを特徴とする請求の範囲第１８項に記載のデータ処理装置。

２０．上記テーブルを記憶するテーブル記憶手段をさらに備える
ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

２１．上記宛先は、上記データを受信すべき通信端末のＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスである
ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

２２．上記データブロックは、ＤＶＢ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｂｒｏａｄｃａｓｔｉｎｇ）の規格に準拠したものである
ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

２３．１チップのＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）で構成される
ことを特徴とする請求の範囲第１２項に記載のデータ処理装置。

２４．データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理方法であって、
宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、
上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定ステップと、
上記判定ステップによる判定結果に基づいて、上記データブロックに配置され

たデータの出力を制御する出力制御ステップと

を備えることを特徴とするデータ処理方法。

２５．データとともに、そのデータの宛先が配置されたデータブロックを、コンピュータに処理させるプログラムが記録されている記録媒体であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、上記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

上記注目エントリに登録された上記エントリ有効情報に基づいて、上記注目エントリが有効かどうかを判定する判定ステップと、

上記判定ステップによる判定結果に基づいて、上記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えるプログラムが記録されている

ことを特徴とする記録媒体。

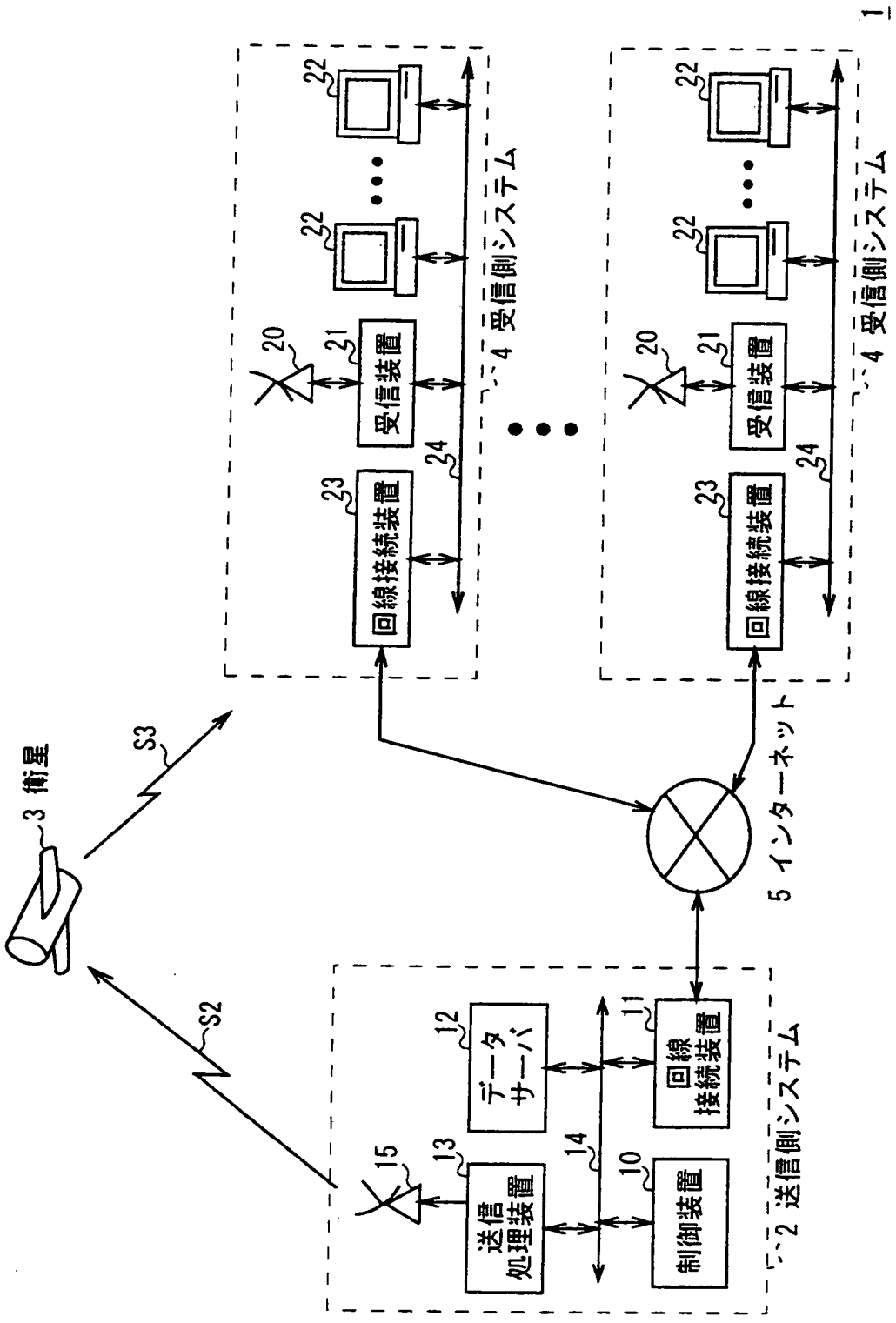

1
2 送信側システム
3 衛星
4 受信側システム
5 インターネット
S2
S3
10 制御装置
11 回線接続装置
12 データサーバ
13 送信処理装置
14
15
20
21 受信装置
22
23 回線接続装置
24

図1

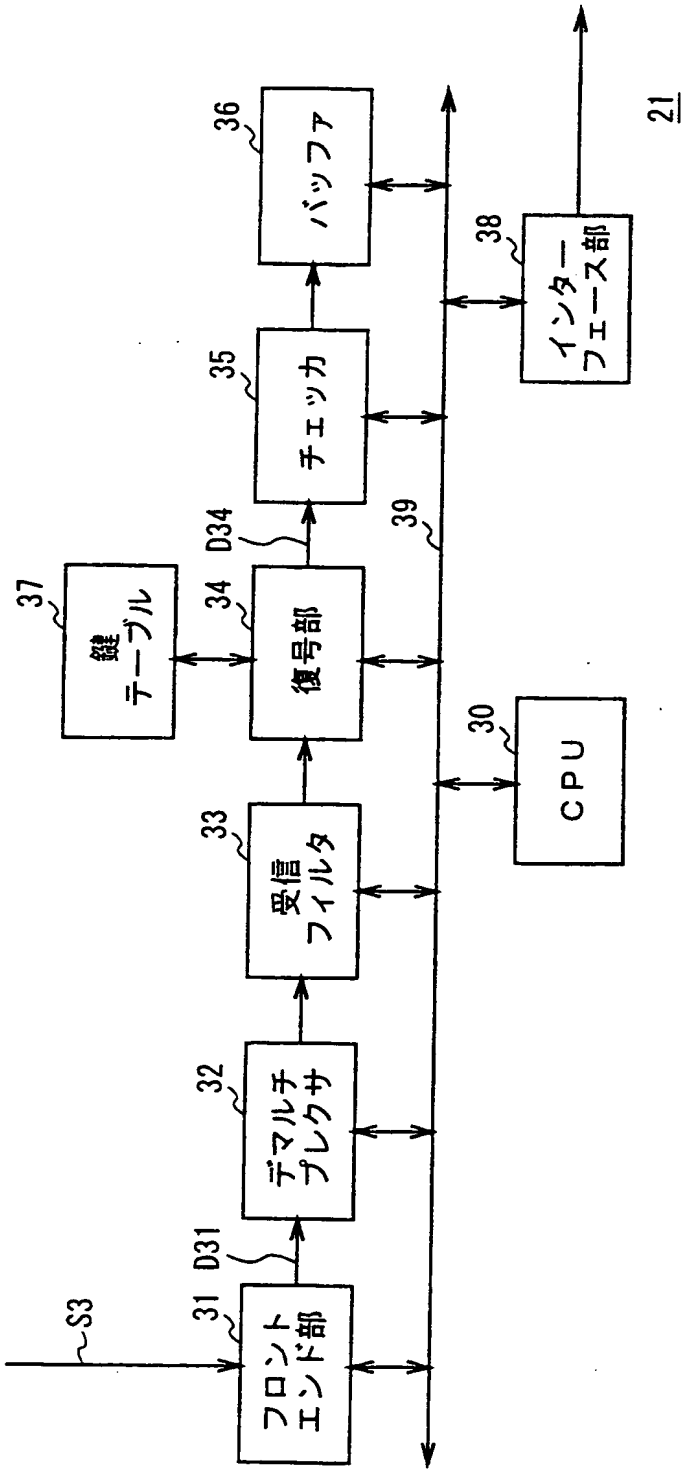

S3
フロントエンド部
31
D31
デマルチプレクサ
32
受信フィルタ
33
復号部
34
D34
チェッカ
35
バッファ
36
鍵テーブル
37
インターフェース部
38
CPU
30
39
21

図2

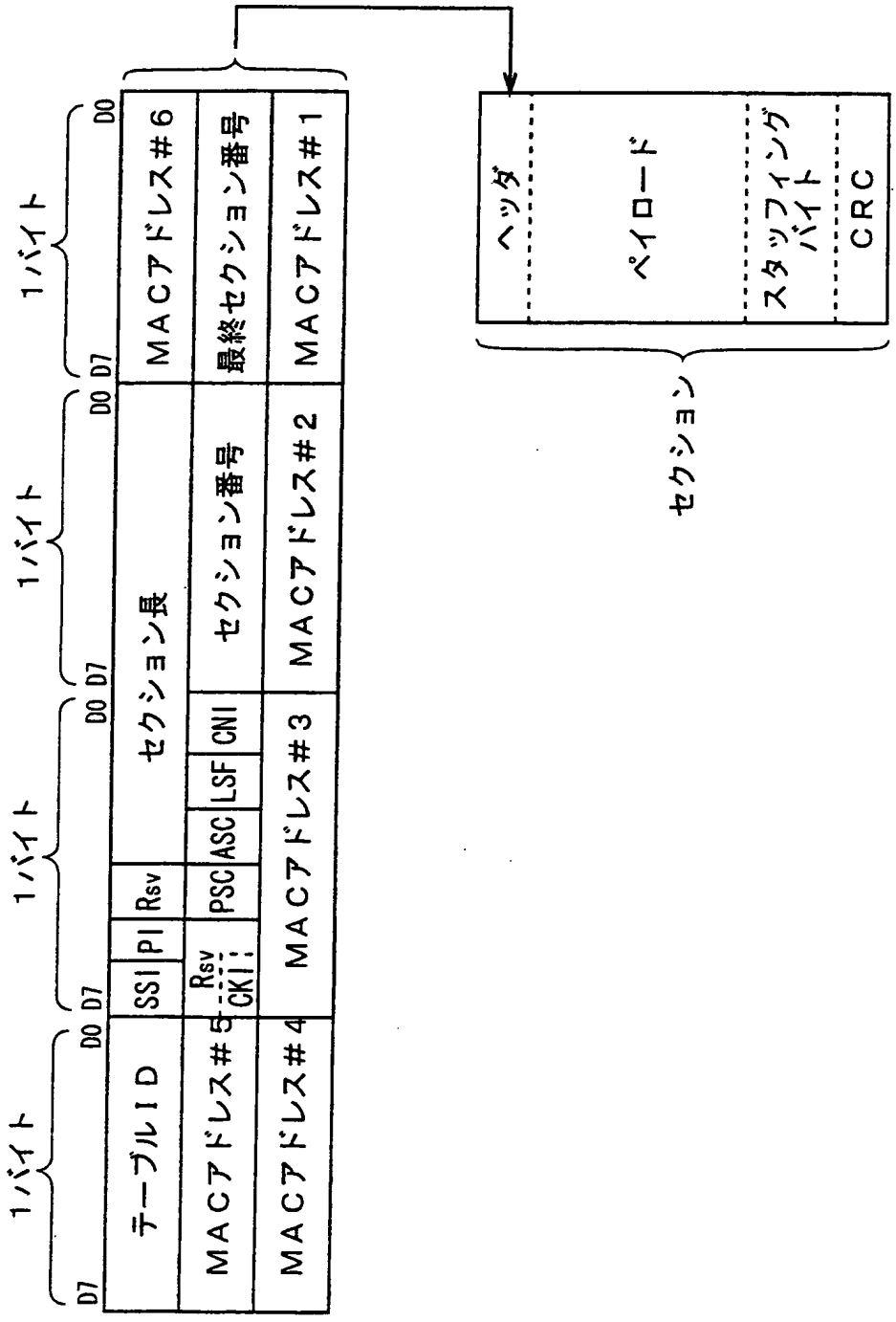

1バイト
D7
D0
テーブルID
MACアドレス#5
MACアドレス#4
SSI
PI
Rsv
Rsv
CKI
PSC
ASC
LSF
CNI
セクション長
セクション番号
MACアドレス#3
MACアドレス#2
最終セクション番号
MACアドレス#1
MACアドレス#6
ヘッダ
ペイロード
スタッフィングバイト
CRC
セクション

図3

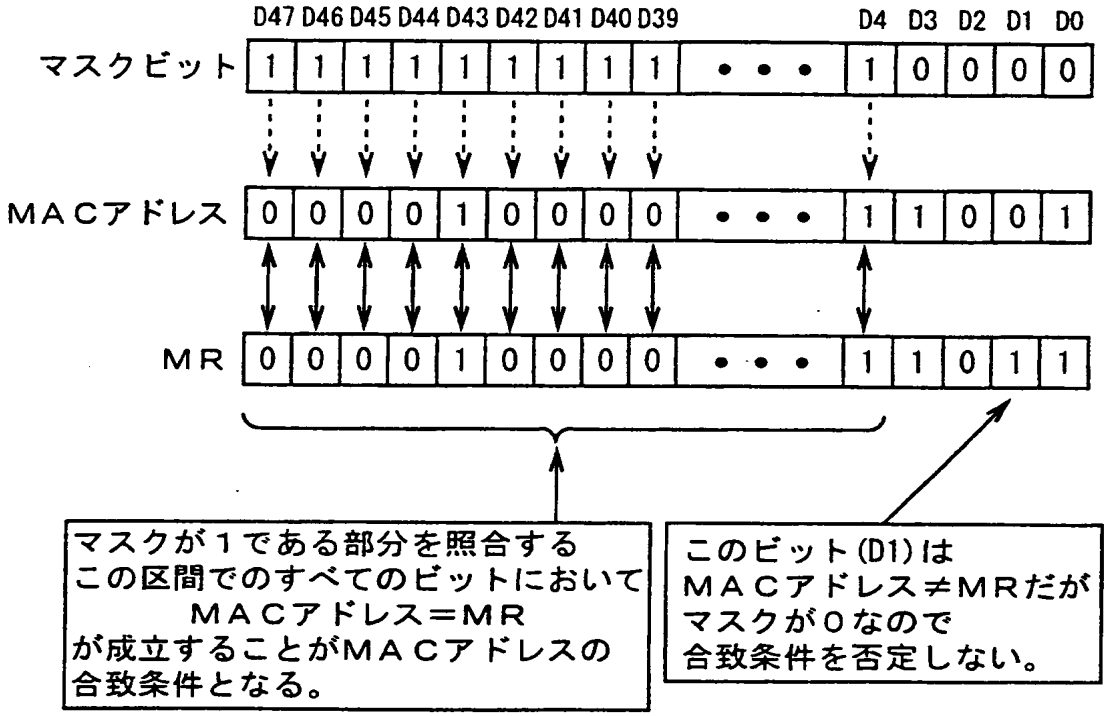

D47 D46 D45 D44 D43 D42 D41 D40 D39
D4 D3 D2 D1 D0
マスクビット
1 1 1 1 1 1 1 1 1 • • • 1 0 0 0 0
MACアドレス
0 0 0 0 1 0 0 0 0 • • • 1 1 0 0 1
MR
0 0 0 0 1 0 0 0 0 • • • 1 1 0 1 1
マスクが１である部分を照合する
この区間でのすべてのビットにおいて
MACアドレス＝MR
が成立することがMACアドレスの
合致条件となる。
このビット(D1)は
MACアドレス≠MRだが
マスクが０なので
合致条件を否定しない。

図４

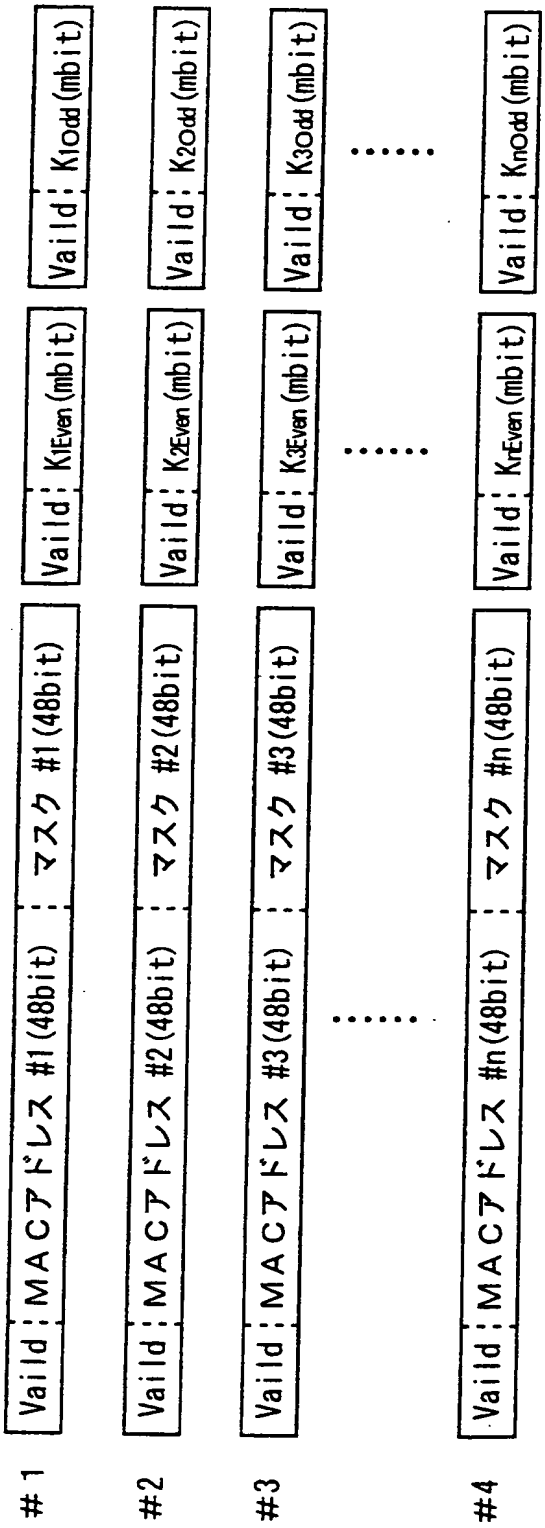

#1
Vaild
MACアドレス #1(48bit)
マスク #1(48bit)
Vaild
K1Even(mbit)
Vaild
K1Odd(mbit)
#2
Vaild
MACアドレス #2(48bit)
マスク #2(48bit)
Vaild
K2Even(mbit)
Vaild
K2Odd(mbit)
#3
Vaild
MACアドレス #3(48bit)
マスク #3(48bit)
Vaild
K3Even(mbit)
Vaild
K3Odd(mbit)
#4
Vaild
MACアドレス #n(48bit)
マスク #n(48bit)
Vaild
KnEven(mbit)
Vaild
KnOdd(mbit)

図5

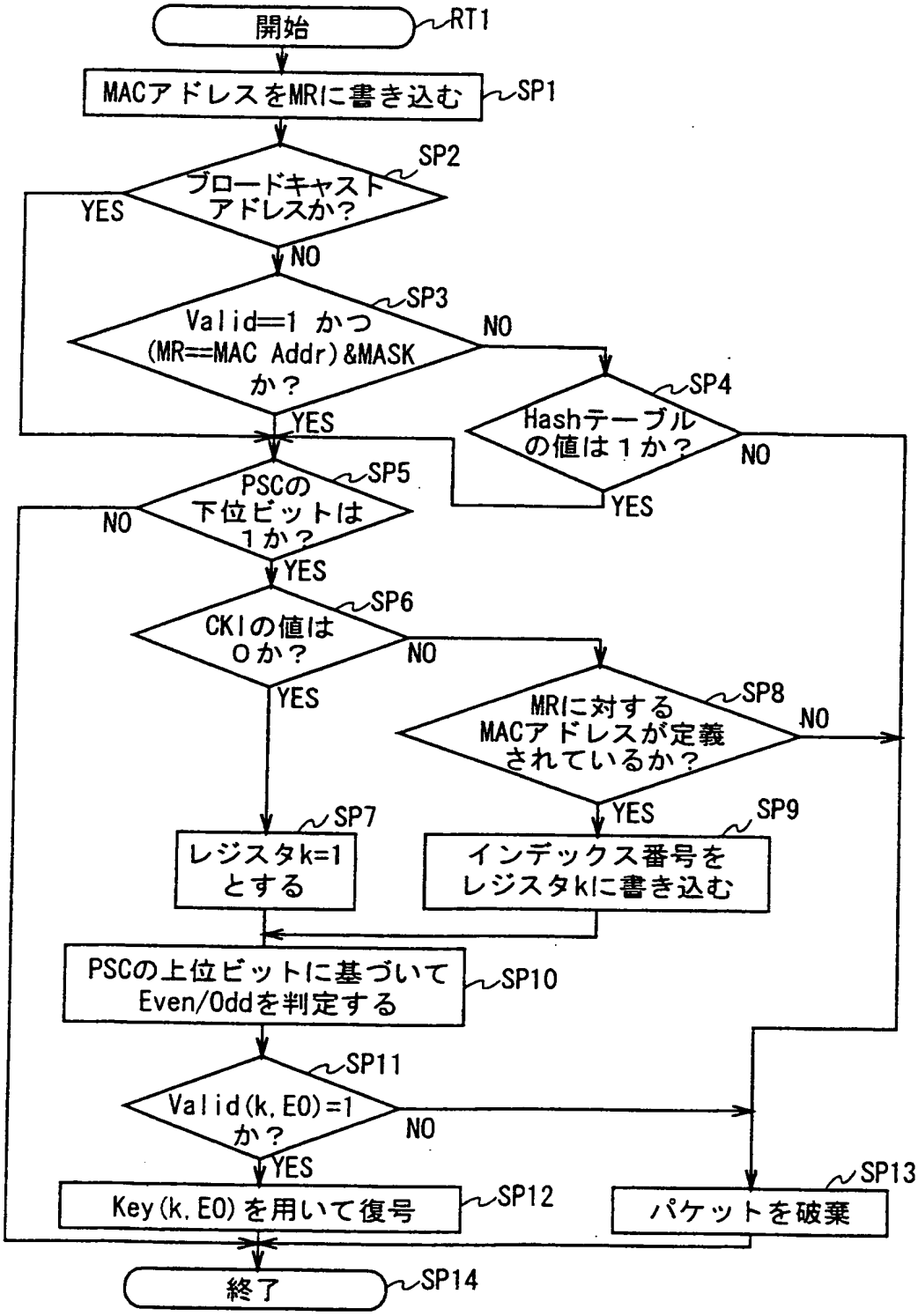

開始
RT1
MACアドレスをMRに書き込む
SP1
ブロードキャスト
アドレスか？
SP2
YES
NO
Valid=1 かつ
(MR==MAC Addr)&MASK
か？
SP3
NO
YES
Hashテーブル
の値は１か？
SP4
NO
YES
PSCの
下位ビットは
１か？
SP5
NO
YES
CKIの値は
０か？
SP6
NO
YES
MRに対する
MACアドレスが定義
されているか？
SP8
NO
YES
レジスタk=1
とする
SP7
インデックス番号を
レジスタkに書き込む
SP9
PSCの上位ビットに基づいて
Even/Oddを判定する
SP10
Valid(k, E0)=1
か？
SP11
NO
YES
Key(k, E0)を用いて復号
SP12
パケットを破棄
SP13
終了
SP14

図６

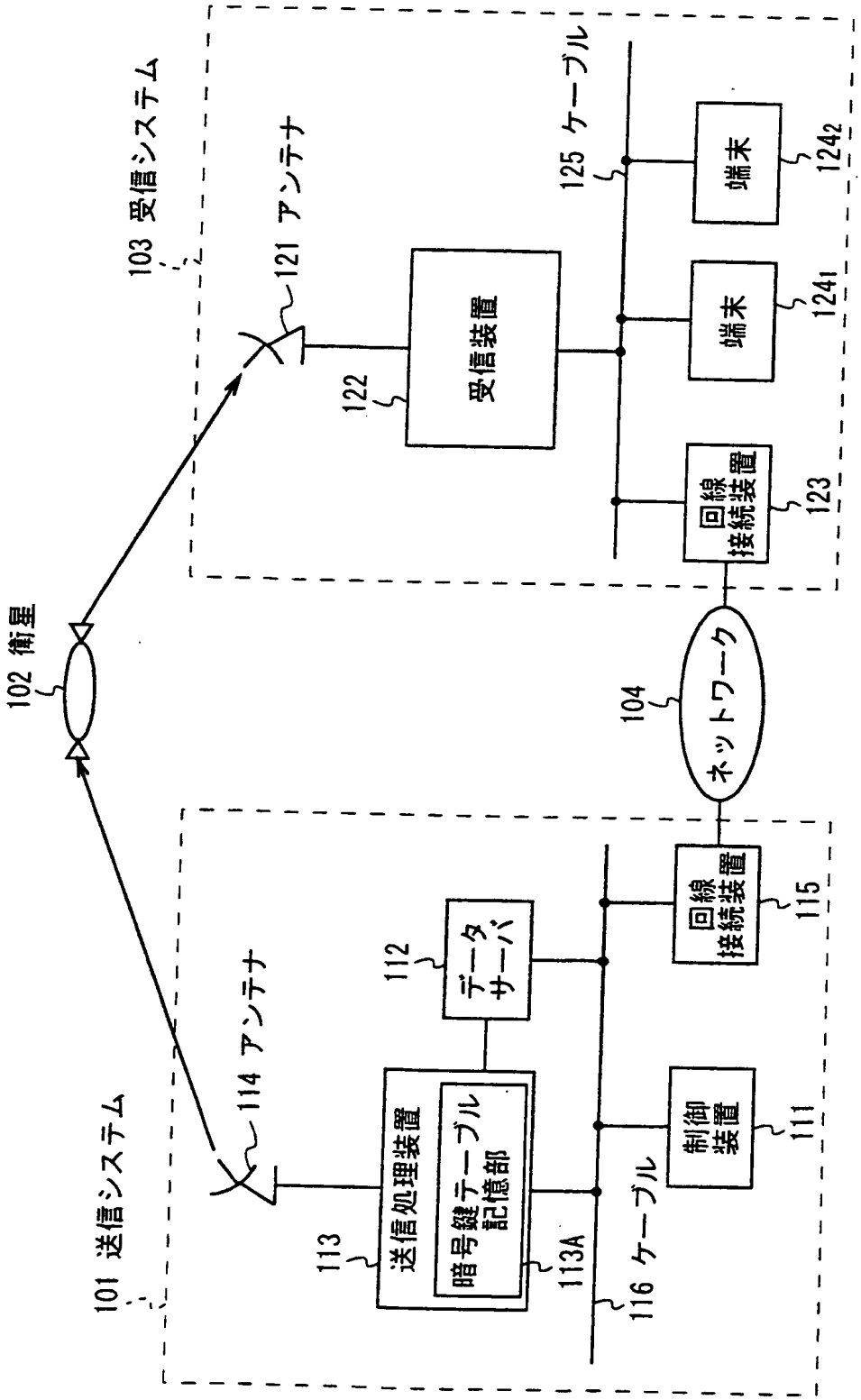

101 送信システム
102 衛星
103 受信システム
104 ネットワーク
111 制御装置
112 データサーバ
113 送信処理装置
113A 暗号鍵テーブル記憶部
114 アンテナ
115 回線接続装置
116 ケーブル
121 アンテナ
122 受信装置
123 回線接続装置
125 ケーブル
1241 端末
1242 端末

図7

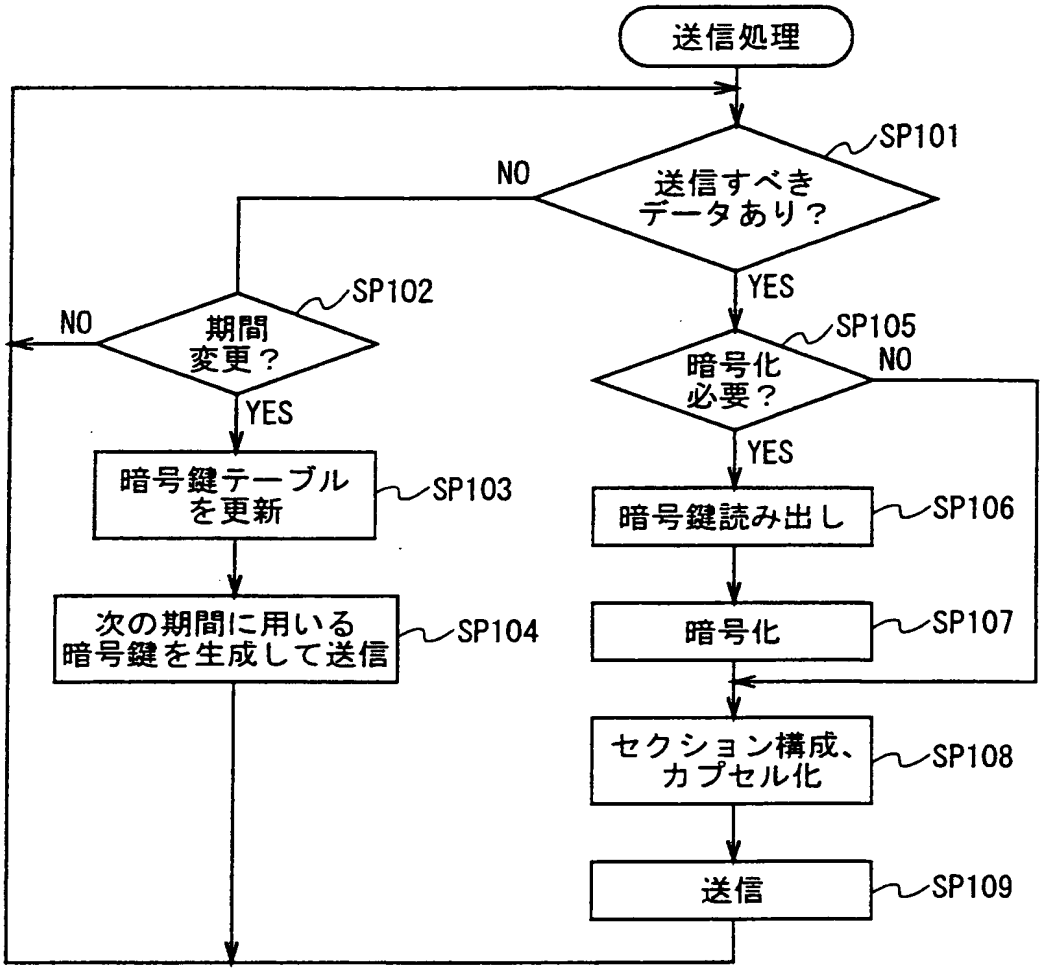

送信処理
SP101
送信すべき
データあり？
NO
YES
SP102
期間
変更？
NO
YES
SP105
暗号化
必要？
NO
YES
暗号鍵テーブル
を更新
SP103
次の期間に用いる
暗号鍵を生成して送信
SP104
暗号鍵読み出し
SP106
暗号化
SP107
セクション構成、
カプセル化
SP108
送信
SP109

図８

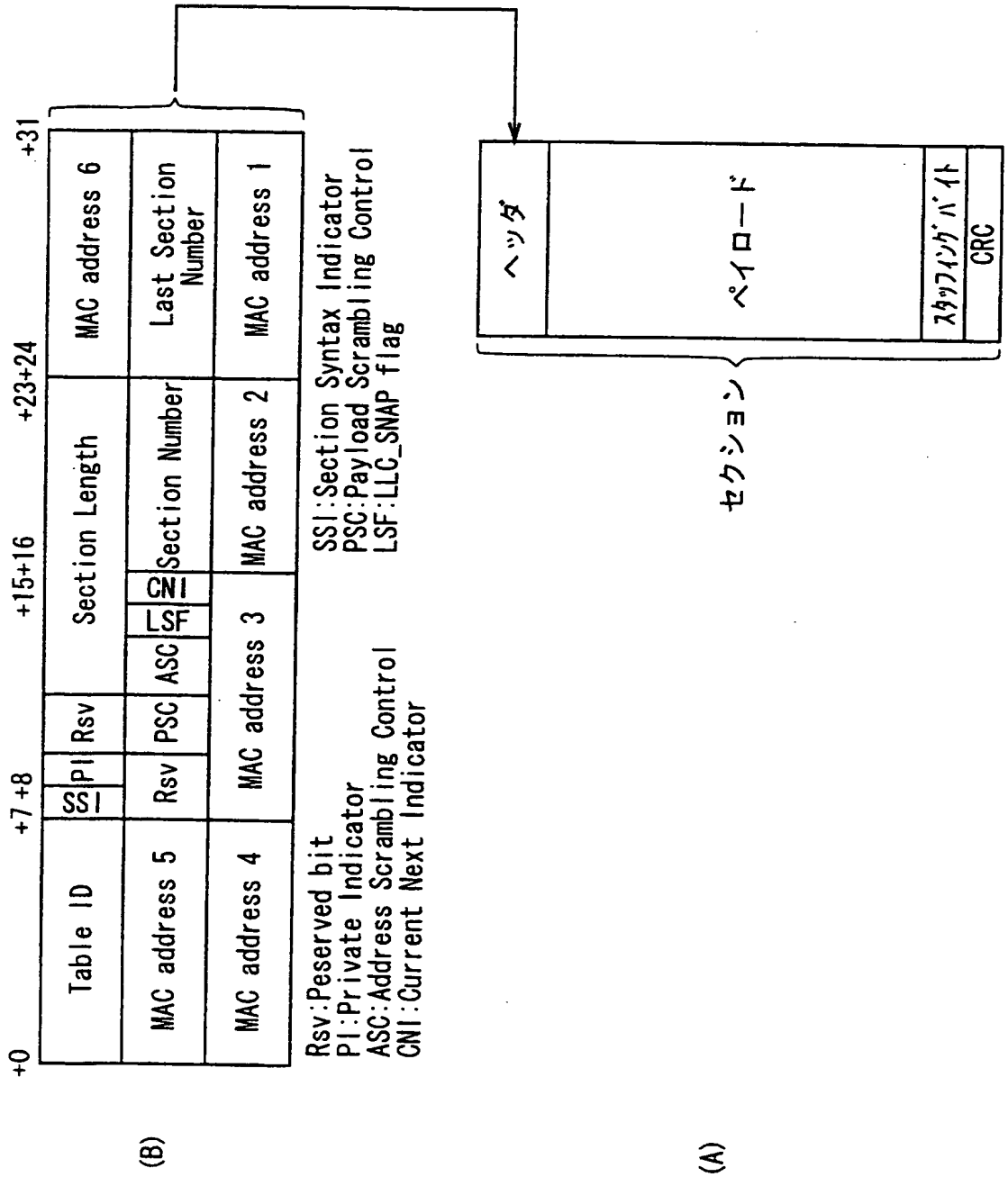

(B)
+0
+7 +8
+15+16
+23+24
+31
Table ID
SSI
PI
Rsv
Section Length
MAC address 6
MAC address 5
Rsv
PSC
ASC
LSF
CNI
Section Number
Last Section Number
MAC address 4
MAC address 3
MAC address 2
MAC address 1
Rsv:Peserved bit
PI:Private Indicator
ASC:Address Scrambling Control
CNI:Current Next Indicator
SSI:Section Syntax Indicator
PSC:Payload Scrambling Control
LSF:LLC_SNAP flag
(A)
ヘッダ
ペイロード
スタッフィングバイト
CRC
セクション

図9

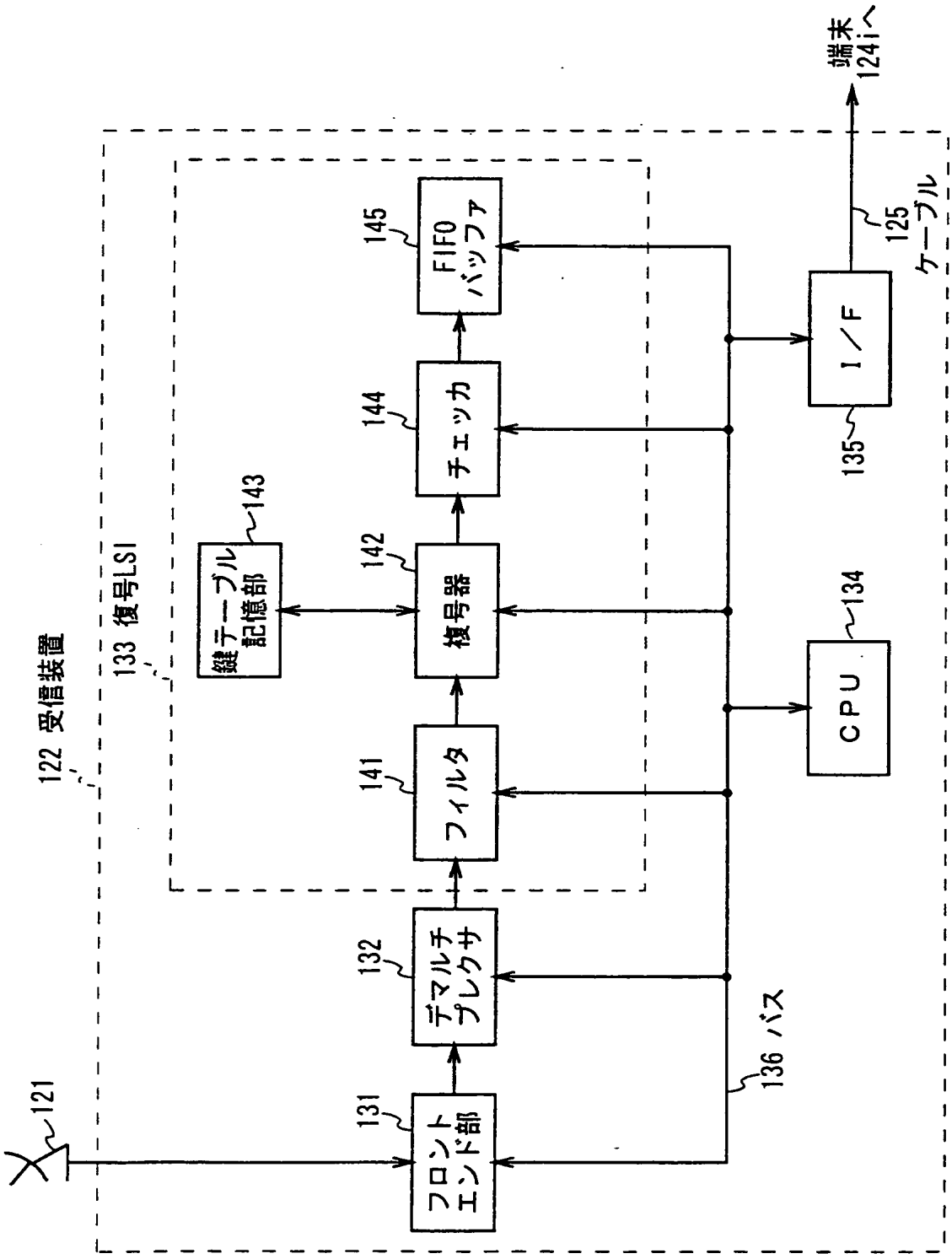

端末
124i へ
125
ケーブル
I／F
135
CPU
134
136 バス
121
122 受信装置
133 復号LSI
フロントエンド部
131
デマルチプレクサ
132
フィルタ
141
復号器
142
鍵テーブル記憶部
143
チェッカ
144
FIFO バッファ
145

図１０

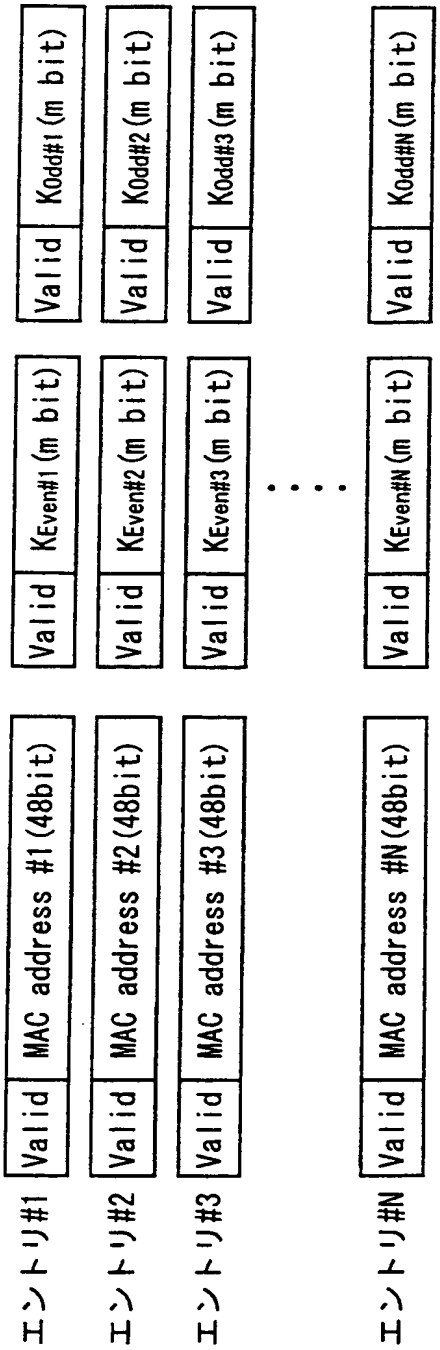

エントリ#1
エントリ#2
エントリ#3
エントリ#N
Valid
MAC address #1(48bit)
MAC address #2(48bit)
MAC address #3(48bit)
MAC address #N(48bit)
Valid
KEven#1(m bit)
KEven#2(m bit)
KEven#3(m bit)
KEven#N(m bit)
Valid
KOdd#1(m bit)
KOdd#2(m bit)
KOdd#3(m bit)
KOdd#N(m bit)

図１１

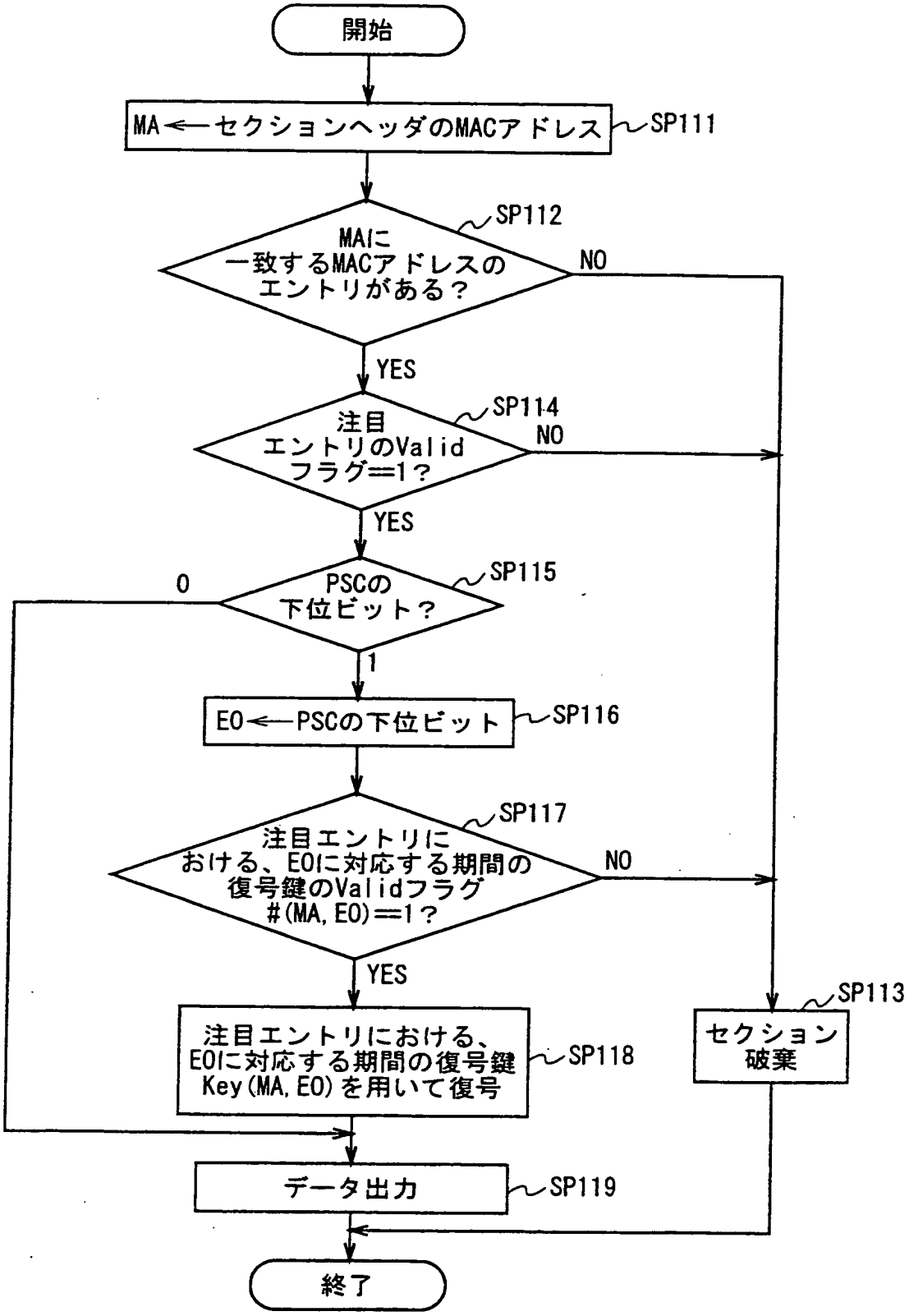

開始
MA←セクションヘッダのMACアドレス
SP111
MAに
一致するMACアドレスの
エントリがある？
SP112
NO
YES
注目
エントリのValid
フラグ=1？
SP114
NO
YES
PSCの
下位ビット？
SP115
0
1
EO←PSCの下位ビット
SP116
注目エントリに
おける、EOに対応する期間の
復号鍵のValidフラグ
#(MA, EO)=1？
SP117
NO
YES
注目エントリにおける、
EOに対応する期間の復号鍵
Key(MA, EO)を用いて復号
SP118
セクション
破棄
SP113
データ出力
SP119
終了

図１２

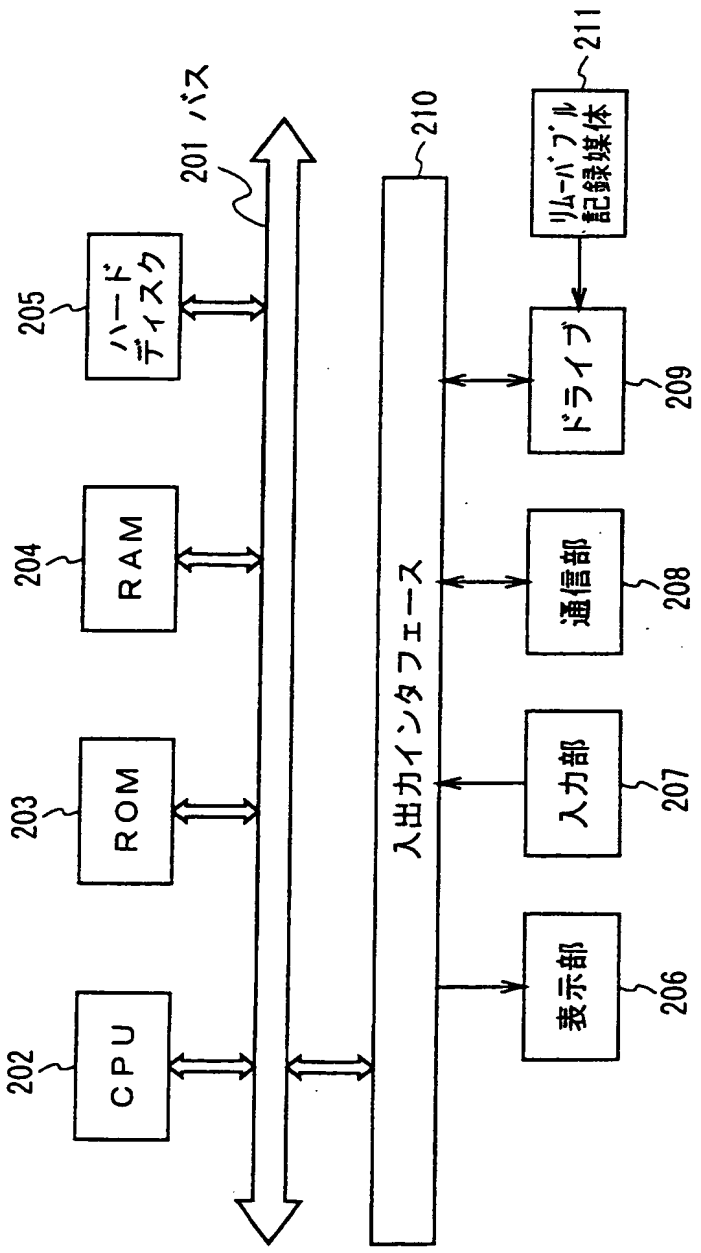

CPU
202
ROM
203
RAM
204
ハードディスク
205
201 バス
入出力インタフェース
210
表示部
206
入力部
207
通信部
208
ドライブ
209
リムーバブル記録媒体
211

図１３

符　号　の　説　明

１……衛星データ伝送システム、２……送信側システム、３……衛星、４……受信側システム、５……インターネット、１０……制御装置、１１……回線接続装置、１２……データサーバ、１３……送信処理装置、１４……ローカルネットワーク、１５……送信アンテナ、２０……受信アンテナ、２１……受信装置、２２……情報処理装置、２３……回線接続装置、２４……ローカルネットワーク、３０……ＣＰＵ、３１……フロントエンド部、３２……デマルチプレクサ、３３……受信フィルタ、３４……復号部、３５……チェッカ、３６……バッファ、３７……鍵テーブル、３８……インターフェース部、３９……バス、１０１……送信システム、１０２……衛星、１０３……受信システム、１０４……ネットワーク、１１１……制御装置、１１２……データサーバ、１１３……送信処理装置、１１３Ａ……暗号鍵テーブル記憶部、１１４……アンテナ、１１５……回線接続装置、１１６……ケーブル、１２１……アンテナ、１２２……受信装置、１２３……回線接続装置、124_1，124_2……端末、１３１……フロントエンド部、１３２……デマルチプレクサ、１３３……復号ＬＳＩ、１３４……ＣＰＵ、１３５……Ｉ／Ｆ、１４１……フィルタ、１４２……復号器、１４３……鍵テーブル記憶部、１４４……チェッカ、１４５……ＦＩＦＯバッファ、２０１……バス、２０２……ＣＰＵ、２０３……ＲＯＭ、２０４……ＲＡＭ、２０５……ハードディスク、２０６……出力部、２０７……入力部、２０８……通信部、２０９……ドライブ、２１０……入出力インタフェース、２１１……リムーバブル記録媒体。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/07682

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/18, H04L9/36, H04L9/32,
H04H1/00, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP, 10-215244, A (Sony Corporation), 11 August, 1998 (11.08.98), Par. Nos. [0046] to [0088], [0102] (Family: none)	1,5,6,9 2-4,7,8,10,11
Y	JP, 10-210066, A (Sumitomo Electric Industries, Ltd.), 07 August, 1998 (07.08.98), Par. Nos. [0008] to [0011] (Family: none)	3,11
Y	EP, 784392, A2 (Mitsubishi Electric Corporation), 16 July, 1997 (16.07.97), Figs. 23, 24 & JP, 9-252294, A & CA, 2194421, A & TW, 315451, A & KR, 98013071, A	4,8
Y	Jeffery Mogul "RFC919", October, 1984 (10.84)	2,7,10
E,A	JP, 2000-312225, A (Hitachi Information Technology Co., Ltd.), 07 November, 2000 (07.11.00), Claim 18 & EP, 993153, A1 & CN, 1250290, A & CA, 2282159, A1	12-25

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 December, 2000 (12.12.00)	19 December, 2000 (19.12.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/07682

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Sony Research Forum 1996 Ronbunshuu, 01 February, 1997 (01.02.97), Tomoyuki ASANO et al., "PRISM Prototype ni okeru Conditional Access System", pp.300-304	1-11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/07682

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-11 relate to control of broadcasting by use of common address.

The inventions of claims 12-25 relate to transmission control by using information concerning validity of entry of address table.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０７６８２

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．　Ｃｌ．[7]　Ｈ０４Ｌ１２／１８，Ｈ０４Ｌ９／３６，Ｈ０４Ｌ９／３２，
Ｈ０４Ｈ１／００，Ｈ０４Ｎ７／１６

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．　Ｃｌ．[7]　Ｈ０４Ｌ１２／１８，Ｈ０４Ｌ９／３６，Ｈ０４Ｌ９／３２，
Ｈ０４Ｈ１／００，Ｈ０４Ｎ７／１６

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２６－１９９６年
日本国公開実用新案公報　１９７１－２０００年
日本国登録実用新案公報　１９９４－２０００年
日本国実用新案登録公報　１９９６－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	ＪＰ，１０－２１５２４４，Ａ（ソニー株式会社），１１．８月．１９９８（１１．０８．９８），段落【0046】～段落【0088】、段落【0102】（ファミリーなし）	１，５，６，９ ２－４，７，８，１０，１１
Y	ＪＰ，１０－２１００６６，Ａ（住友電気工業株式会社），７．８月．１９９８（０７．０８．９８），段落【0008】～段落【0011】（ファミリーなし）	３，１１

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１２．１２．００	19.12.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	土居　仁士	５Ｘ	９３７１
	電話番号　０３－３５８１－１１０１　内線　３５９４		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０７６８２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＥＰ，７８４３９２，Ａ２（三菱電機株式会社），１６．７月．１９９７（１６．０７．９７），図２３，図２４　＆ＪＰ，９－２５２２９４，Ａ　＆ＣＡ，２１９４４２１，Ａ　＆ＴＷ，３１５４５１，Ａ　＆ＫＲ，９８０１３０７１，Ａ	４，８
Ｙ	Jeffery Mogul「RFC919」，１０月．１９８４（１０．８４）	２，７，１０
Ｅ，Ａ	ＪＰ，２０００－３１２２２５，Ａ（株式会社インフォメーションテクノロジー），７．１１月．２０００（０７．１１．００），請求項１８　＆ＥＰ，９９３１５３，Ａ１　＆ＣＮ，１２５０２９０，Ａ　＆ＣＡ，２２８２１５９，Ａ１	１２－２５
Ａ	ソニーリサーチフォーラム１９９６論文集，１．２月．１９９７（０１．０２．９７），浅野智之他，「ＰＲＩＳＭプロトタイプにおけるコンディショナルアクセスシステム」，ｐ．３００－３０４	１－１１

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０７６８２

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－１１は、共通アドレスの利用による同報の制御に関するものである。

請求の範囲１２－２５は、宛先テーブルのエントリの有効情報による送信制御に関するものである。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。